

No. 19-2265

In the
United States Court of Appeals
for the Fourth Circuit

PUBLIC INTEREST LEGAL FOUNDATION,
Plaintiff-Appellant,

v.

NORTH CAROLINA STATE BOARD OF ELECTIONS
And KAREN BRINSON BELL, in her official capacity as Executive Director of
the North Carolina State Board of Elections,
Defendants-Appellees.

On Appeal from the United States District Court
for the Eastern District of North Carolina

BRIEF OF DEFENDANTS-APPELLEES

JOSHUA H. STEIN
Attorney General

Ryan Y. Park
Deputy Solicitor General

Caryn Devins Strickland
Solicitor General Fellow

Paul M. Cox
Special Deputy Attorney General

North Carolina Department of Justice
Post Office Box 629
Raleigh, North Carolina 27602
(919) 716-6400

Counsel for Defendants-Appellees

CORPORATE DISCLOSURE STATEMENT

I certify, pursuant to Federal Rule of Appellate Procedure 26.1 and Local Rule 26.1, that no appellee is in any part a publicly held corporation, a publicly held entity, or a trade association, and that no publicly held corporation or other publicly held entity has a direct financial interest in the outcome of this litigation.

Dated: February 12, 2020

/s/ Ryan Y. Park
Ryan Y. Park

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES.....	iv
ISSUES PRESENTED	1
STATEMENT OF CASE	2
A. The Board Used Confidential Information from Government Agencies to Investigate Citizenship Status.....	4
1. The Board used confidential DMV information.....	5
2. The Board used confidential information provided by the federal government	7
3. The Board investigated registered voters.....	10
B. PILF Demanded Confidential Information on Potential Noncitizens	12
C. The Board Complied with PILF’s Requests to the Extent Allowed by Law	15
D. PILF Filed This Lawsuit Against the Board.....	18
SUMMARY OF THE ARGUMENT	20
ARGUMENT	22
I. The District Court Correctly Held That The NVRA Does Not Require The Board To Disclose The Withheld Documents	22
A. Courts Apply a Strong Presumption that Congress Did Not Intend to Compromise Individual Privacy	22

- B. PILF Cannot Show that the NVRA Clearly Requires the Board to Disclose the Withheld Documents.....26
 - i. The text of the NVRA does not require disclosure of personally sensitive information26
 - ii. The structure of the NVRA shows that Congress was focused on government transparency, not exposing voters’ private information30
 - iii. Disclosing the withheld information would undermine the NVRA’s purpose 33
- II. The Withheld Records Are Protected From Disclosure By Federal Privacy Laws.....38
 - A. The NVRA and Federal Privacy Laws Must Be Read Together as an Inclusive Whole39
 - B. The Driver Privacy Protection Act Bars Disclosure of the Withheld Documents 40
 - C. The Privacy Act Also Bars Disclosure of the Withheld Documents45
 - D. PILF Cannot Show that Congress Intended the NVRA to Displace All Other Privacy Laws.....50
- III. PILF’s Expansive Reading Of NVRA Section 8(i) Would Raise Serious Doubts About The Statute’s Constitutionality 55
 - A. The Supreme Court and This Court Have Long Recognized a Constitutional Right to Informational Privacy56
 - B. Disclosing the Private Information Requested by PILF Would Violate the Constitution 64

C. PILF’s Requests Are Also Invalid Because They Undermine
Other Fundamental Constitutional Rights..... 66

CONCLUSION 71

CERTIFICATE OF SERVICE

CERTIFICATE OF COMPLIANCE

Addendum Addendum 1

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Arcia v. Florida Secretary of State</i> , 772 F.3d 1335 (11th Cir. 2014)	38
<i>Branch v. Smith</i> , 538 U.S. 254 (2003)	39
<i>Campbell v. Acuff-Rose Music, Inc.</i> , 510 U.S. 569 (1994)	43
<i>City of Cleburne, Tex. v. Cleburne Living Ctr.</i> , 473 U.S. 432 (1985)	69
<i>Crandon v. United States</i> , 494 U.S. 152 (1990)	34
<i>Dahlstrom v. Sun-Times Media, LLC</i> , 777 F.3d 937 (7th Cir. 2015).....	43, 44
<i>Douglas Oil Co. v. Petrol Stops Northwest</i> , 441 U.S. 211 (1979)	65, 66
<i>Elec. Welfare Tr. Fund v. United States</i> , 907 F.3d 165 (4th Cir. 2018)	39
<i>FDA v. Brown & Williamson Tobacco Corp.</i> , 529 U.S. 120 (2002)	30
<i>Gaines Motor Lines, Inc. v. Klaussner Furniture Indus., Inc.</i> , 734 F.3d 296 (4th Cir. 2013)	33, 34
<i>Goodyear Atomic Corp. v. Miller</i> , 486 U.S. 174 (1988)	41

<i>Greidinger v. Davis</i> , 998 F.2d 1344 (4th Cir. 1993)	<i>passim</i>
<i>Gustafson v. Alloyd Co.</i> , 513 U.S. 561 (1995)	31
<i>Hancock v. County of Rensselaer</i> , 882 F.3d 58 (2d Cir. 2018)	64
<i>In re Crawford</i> , 194 F.3d 954 (9th Cir. 1999)	64
<i>In re Sealed Matter</i> , No. [SEALED], Doc. [SEALED] (E.D.N.C. Dec. 12, 2019)	17
<i>INS v. St. Cyr</i> , 533 U.S. 289 (2001)	55
<i>Lake v. Neal</i> , 585 F.3d 1059 (7th Cir. 2009)	41, 43
<i>Maracich v. Spears</i> , 570 U.S. 48 (2013)	<i>passim</i>
<i>Mellouli v. Lynch</i> , 135 S. Ct. 1980 (2015)	27, 28
<i>Moore v. Kobach</i> , 359 F.Supp.3d 1029 (D. Kan. 2019)	69
<i>NAACP v. Alabama</i> , 357 U.S. 449 (1958)	67
<i>NASA v. Nelson</i> , 562 U.S. 134 (2011)	60, 61

<i>National Archives and Records Admin. v. Favish</i> , 541 U.S. 157 (2004).....	36
<i>National Magazine, Washington Bureau v. U.S. Customs Service</i> , 71 F.3d 885 (D.C. Cir. 1995).....	65
<i>Nixon v. Administrator of General Services</i> , 433 U.S. 425 (1977)	60
<i>Olmstead v. United States</i> , 277 U.S. 438 (1928)	56
<i>Pesce v. J. Sterling Morton High School</i> , 830 F.2d 789 (7th Cir. 1987).....	64
<i>Project Vote v. Kemp</i> , 208 F. Supp. 3d 1320 (N.D. Ga. 2016)	53
<i>Project Vote v. Long</i> , 752 F. Supp. 2d 697 (E.D. Va 2010)	35
<i>Project Vote v. Long</i> , 682 F.3d 331 (4th Cir. 2012)	22, 23, 28, 29, 30, 36, 37
<i>Pub. Interest Legal Found. v. Boockvar</i> , No. 1:19-CV-622, 2019 WL 6828620 (M.D. Pa. Dec. 13, 2019)	42, 45, 53
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	59
<i>Ruckelshaus v. Monsanto Co.</i> , 467 U.S. 986 (1984)	46
<i>Schneider v. Rusk</i> , 377 U.S. 163 (1964).....	70

<i>Siegler v. Best Buy Co. of Minn.,</i> 519 F. App'x 604 (11th Cir. 2013)	43
<i>Stern v. FBI,</i> 737 F.2d 84 (D.C. Cir. 1984)	25, 33
<i>Taylor v. Acxiom Corp.,</i> 612 F.3d 325 (5th Cir. 2010)	40
<i>Taylor v. Best,</i> 746 F.2d 220 (4th Cir. 1984)	57, 63
<i>Tex. Democratic Party v. Bettencourt</i> , No. H-08-3332, 2009 U.S. Dist. LEXIS 133441 (S.D. Tex. July 16, 2009)	30, 35, 50, 53, 54, 55
<i>Tex. League of United Latin Am. Citizens et al v. Whitley, et al,</i> No. 5:19-cv-00074-FB, Doc. 61 (W.D. Tex. Feb 27, 2019)	6, 69
<i>Trentadue v. Integrity Committee,</i> 501 F.3d 1215 (10th Cir. 2007)	33
<i>True the Vote v. Hosemann,</i> 43 F. Supp. 3d 693 (S.D. Miss. 2014)	24, 35, 36, 50, 53, 54
<i>U.S. Dep't of Justice v. Reporters Comm. For Freedom of Press,</i> 489 U.S. 749 (1989)	32, 33, 45, 65
<i>United States v. Banker,</i> 876 F.3d 530 (4th Cir. 2017)	39
<i>United States v. Briggs,</i> 514 F.2d 794 (5th Cir. 1975)	25, 35
<i>United States v. Coughlan,</i> 842 F.2d 737 (4th Cir. 1988)	52, 65

<i>United States v. Florida</i> , 870 F. Supp. 2d 1346 (N.D. Fla. 2012)	6, 69
<i>United States v. Hastie</i> , 854 F.3d 1298 (11th Cir. 2017)	44
<i>United States v. Jones</i> , 132 S. Ct. 945 (2012)	56
<i>United States v. Westinghouse Elec. Corp.</i> , 638 F.2d 570 (3d Cir. 1980)	64
<i>Wachovia Bank v. Schmidt</i> , 546 U.S. 303 (2006)	39, 40
<i>Walls v. City of Petersburg</i> , 895 F.2d 188 (4th Cir. 1990)	56, 57, 62, 63
<i>Whalen v. Roe</i> , 429 U.S. 589 (1977)	21, 51, 56, 57, 58, 59
<i>Whitman v. American Trucking Ass’n</i> , 531 U.S. 457 (2001)	51
<i>Woodland v. Houston</i> , 940 F.2d 134 (5th Cir. 1991)	64
<i>Yates v. United States</i> , 135 S. Ct. 1074 (2015)	28
<i>Zadvydas v. Davis</i> , 533 U.S. 678 (2001)	55
<i>Zobel v. Williams</i> , 457 U.S. 55 (1982)	70

Constitutional Provision

U.S. Const. am. XIV, § 1..... 69

Statutes

5 U.S.C. § 552..... 51

5 U.S.C. § 552a..... 46, 47

18 U.S.C. § 611 18

18 U.S.C. § 2721..... 41, 42, 44, 45

18 U.S.C. § 272541, 42, 43

52 U.S.C. § 205012, 13, 34

52 U.S.C. § 20503..... 14

52 U.S.C. § 20504 31, 41

52 U.S.C. § 20505.....31

52 U.S.C. § 2050631

52 U.S.C. § 20507.....*passim*

52 U.S.C. § 2050831

N.C. Gen. Stat. § 75-6652

N.C. Gen. Stat. § 132-1.452

N.C. Gen. Stat. § 163-22(d) 2, 11

Rule

Fed. R. Civ. P. 5.2.....52

Regulation

18 C.F.R. § 17.2252

Other Authorities

Dep't of Homeland Sec., Privacy Impact Assessment for the SAVE Program 2 (2011), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_save.pdf47

DHS & U.S.C.I.S., SAVE Program Guide, at 10, 19 (revised Mar. 2019), <https://save.uscis.gov/web/media/resourcesContents/SAVEProgramGuide.pdf>8, 47

Governor Roy Cooper Objections and Veto Message, S. Bill 250 (Nov. 6, 2019), <https://webservices.ncleg.gov/ViewBillDocument/2019/6866/o/S250-BD-NBC-8368> 12

H. Rep. No. 103-9 (1993) 34, 35

H.R. Rep. No. 93-1416 (1974)45

Identity Theft, FBI, <https://www.fbi.gov/investigate/white-collar-crime/identity-theft> (last visited Feb. 11, 2020)25

S. Rep. No. 103-6 (1993)*passim*

Tim Hoover, *Noncitizen voters ID'd fraction of those first alleged by Gessler*, DENVER POST (Sep. 15, 2012), <https://www.denverpost.com/2012/09/15/noncitizen-voters-idd-fraction-of-those-first-alleged-by-gessler/>7

ISSUE PRESENTED

Is the North Carolina State Board of Elections required to publicly disclose the identities and personal information of registered voters who were once identified as possible noncitizens?

STATEMENT OF THE CASE

Congress enacted the National Voter Registration Act (NVRA) to “promote the exercise” of the right to vote and to overcome “discriminatory and unfair registration laws and procedures.” 52 U.S.C. § 20501(a)(2)-(3). To these ends, the NVRA requires states to expand voter-registration opportunities. It also imposes strict limits on states’ ability to purge eligible voters from the voting rolls.

The North Carolina State Board of Elections is an independent state agency charged with overseeing elections in North Carolina. Under the NVRA, the Board has a duty to prevent the State from unlawfully removing voters from the rolls. In addition, under state law, the Board is charged with investigating election “frauds and irregularities.” N.C. Gen. Stat. § 163-22(d). The Board reports election-law violations to the Attorney General and criminal prosecutors. *Id.*

As part of these duties, the Board has investigated registered voters who may *possibly* be noncitizens. For instance, after the 2016 election, the Board conducted an audit using state and federal computer databases. J.A. 25-58. The audit identified 41 noncitizens who cast ballots; 34 citizens who the computer databases mistakenly identified as noncitizens; and 61 voters

whose investigations were still ongoing when the audit was published.

J.A. 27, 29-30. The Board publicly disclosed the audit's findings. *See* J.A. 10-11, 25-58.

This transparency was not enough for the Public Interest Law Foundation. PILF is a nonprofit organization that uses public-records laws to gather information on voters that it claims are not citizens. J.A. 101-04. PILF produces reports that describe this information in sensational ways, and then disseminates the reports widely to the national media. J.A. 107-15. In 2016, for example, PILF published a report called "Alien Invasion" in which it falsely identified specific voters as noncitizens, accused them of committing voting-related felonies, and published their sensitive personal data, including their social security numbers. J.A. 106-15. Because of these tactics, PILF has been sued for defamation and violations of voting-rights laws. J.A. 100-86.

In 2018, PILF requested from the Board "[d]ocuments regarding all registrants who were identified as potentially not satisfying the citizenship requirements for registration." J.A. 78; *see* J.A. 59-78. PILF demanded that the Board publicly disclose the identities of registered voters who were flagged by computer databases as possible noncitizens—information that

would publicly tar those individuals as suspected felons. PILF also demanded sensitive personal documents that voters provided to confirm their citizenship, including birth certificates and passports. J.A. 59-78. PILF claimed that it was entitled to this information under the NVRA.

In response to PILF's request, the Board provided the full 2016 audit report. J.A. 82-84. The Board also pointed PILF to comprehensive, publicly available data on voters who had been removed from the rolls, as well as voter-history profiles for every registered voter in the State. J.A. 82.

The Board explained, however, that it could not comply with PILF's requests to disclose the identities and personal information of registered voters who were flagged as possible noncitizens. As the Board explained, disclosing that information would violate federal law. J.A. 83-84.

A. The Board Used Confidential Information from Government Agencies to Investigate Citizenship Status.

When investigating whether registered voters might be noncitizens, the Board has undertaken a three-step process. J.A. 33-34.

At each step, the Board relied on confidential, personally sensitive records held in government databases:

- First, the Board used an automated computer process to check voter records against motor-vehicle records held by the North Carolina DMV.
 - Second, the Board used a computer program operated by the U.S. Department of Homeland Security to run matches from the DMV process against confidential immigration and border records held by the federal government.
 - Third, the Board investigated any voters who were flagged as potential noncitizens through these automated programs.
- Voters could verify their citizenship by sending the Board official documents, such as birth certificates and naturalization documents, that prove they are citizens.

Each of these three steps is described in more detail below.

1. The Board used confidential DMV information.

The first step in the Board's process of verifying voter citizenship was to obtain records from the North Carolina DMV. J.A. 33, 82-83. The Board agreed to keep these DMV records confidential.

The Board identified potential noncitizens by checking voter lists against records of DMV customers whose “driver’s license contains a restriction code related to their non-citizen status.” J.A. 208. That code is often generated when a license-holder reports that she is a noncitizen when she applies for a license. When a person becomes a citizen, the code therefore becomes outdated and inaccurate. The code is also sometimes included in error from the outset. *See* J.A. 209.

The 2016 audit found that DMV records were hopelessly inaccurate. Of the voters who were marked as noncitizens in DMV records, 97.6% of them were actually U.S. citizens. J.A. 209.

Other states’ experiences confirm the danger of relying on DMV records to identify noncitizen voters. In Texas, for example, a federal district court halted a purge of 95,000 voters identified based on DMV records after only 80 voters were confirmed to be noncitizens. *Tex. League of United Latin Am. Citizens et al v. Whitley, et al*, No. 5:19-cv-00074-FB, Doc. 61 at 4, (W.D. Tex. Feb 27, 2019). Similarly, in Florida, an initial DMV-based list of 180,000 alleged noncitizens was reduced to a mere 85 ineligible voters. *Id.* at 2 n.3; *United States v. Florida*, 870 F. Supp. 2d 1346, 1347-48 (N.D. Fla. 2012). And

in Colorado, the State demanded proof of citizenship from 4,000 voters based on DMV records, but only 35 voters were actually noncitizens.¹

Given the notorious unreliability of DMV records, those records merely served as a starting point for the Board's investigation.

The Board also used DMV records to learn voters' personally identifying information that license-holders supply on their license applications. J.A. 83. Then, as explained below, the Board entered this personal information into other government databases to narrow the range of voters who are flagged as possible noncitizens.

2. The Board used confidential information provided by the federal government.

The next step in the Board's verification process was to compare the voters identified by the DMV against electronic databases held by the federal government.

The Board has access to these federal databases through its participation in the Systematic Alien Verification for Entitlements (SAVE)

¹ Tim Hoover, *Noncitizen voters ID'd fraction of those first alleged by Gessler*, DENVER POST (Sep. 15, 2012), <https://www.denverpost.com/2012/09/15/noncitizen-voters-idd-fraction-of-those-first-alleged-by-gessler/>.

Program. J.A. 33-34. The SAVE Program is an information-sharing program that allows government agencies to access a number of confidential databases maintained by two federal agencies, the Department of Homeland Security (DHS) and the U.S. Citizenship and Immigration Service (USCIS).

The records used by the SAVE Program are often unreliable or outdated. Like DMV records, the underlying federal databases used by the SAVE Program do not always reflect up-to-date citizenship information. J.A. 209. A particular database might become out of date when, for example, a green-card holder becomes a naturalized citizen. As another example, when noncitizen minors become citizens when they are adopted, they may still be flagged as noncitizens in SAVE. J.A. 209. For these reasons, the 2016 audit report explained that “data matches alone are not sufficient to verify citizenship or to take action against the voters without follow-up investigations.” J.A. 30.

Indeed, the federal government itself admits that SAVE databases cannot, by themselves, confirm whether a person is a citizen.² In fact, the

² DHS & U.S.C.I.S., SAVE Program Guide, at 10, 19 (revised Mar. 2019), <https://save.uscis.gov/web/media/resourcesContents/SAVEProgramGuide.pdf>.

Board's audit revealed that, of the individuals who were flagged in SAVE databases, around 75% of them were actually citizens. J.A. 209.

To use the SAVE Program, the Board must agree to keep all information it receives from the database searches strictly confidential.

J.A. 83. Specifically here, the Board entered into a memorandum of agreement with the federal government that governs the Board's use of federal information. J.A. 190-99. The agreement expressly requires the Board to safeguard the information's confidentiality. *Id.* Among other restrictions, the agreement requires the Board to:

- use information “solely for the purpose of determining” eligibility to vote;
- “[s]afeguard . . . information and access methods” to ensure it is not used for any other purpose;
- “protect [the information’s] confidentiality,” including by seeking “prior written consent” of the federal government before disclosing it;
- “[c]omply with the Privacy Act,” including “in conducting verification procedures” and “in safeguarding, maintaining, and disclosing any data provided or received.”

J.A. 193-94.

In addition, under the agreement, the Board explicitly “acknowledges that the information it receives from DHS-USCIS is governed by the Privacy Act.” J.A. 197. The Board also agreed that improper disclosures of confidential information may result in “criminal penalties.” J.A. 197.

Besides these privacy protections, the agreement provides additional safeguards against misuse of confidential data. For instance, the agreement bars the Board from “discriminatory use of the SAVE program based upon . . . national origin.” J.A. 194. The agreement also observes that the agreement cannot displace the Board’s obligations under federal civil-rights laws. J.A. 198.

3. The Board investigated registered voters.

After the automated database checks, the Board moved to the third step of its verification procedure: investigating possible noncitizens who voted in the 2016 general election.

The Board sent a letter to voters explaining that DMV and DHS data indicate that they may not be U.S. citizens. The letter states that it is a crime for noncitizens to vote. J.A. 53.

The letter requested that voters return a form that admits or denies that they are noncitizens. To prove citizenship, the voter was asked to include “a copy of an official document” that confirmed their citizenship. J.A. 53. Examples of acceptable documents included birth certificates, passports, certificates of naturalization, and certificates of citizenship. J.A. 53-54.

If the voter affirmed that she was *not* a citizen, she was removed from the voter rolls. J.A. 54. The Board could also refer cases for prosecution. See N.C. Gen. Stat. § 163-22(d).

Like the first two steps, this third step cannot definitively verify citizenship status. As the audit report recognized, some citizens may lack supporting documentation. J.A. 30. For instance, some voters became citizens through “derived citizenship” as the children of naturalized citizens. However, to obtain paperwork that shows that changed status, a voter must specifically request it from the federal government—and pay an application fee of \$1170. J.A. 30.

In sum, the Board received information on potential noncitizen voters through three sources: (1) the DMV; (2) the SAVE Program; and (3) the Board’s own investigation.

B. PILF Demanded Confidential Information on Potential Noncitizens.

In the fall of 2018, amid a busy election season, PILF demanded that the Board disclose information regarding “registrations belonging to individuals who do not satisfy the citizenship requirements for voting.”

J.A. 78; *see also* J.A. 59-68.

In its request, PILF demanded three categories of records:

- Documents regarding registrants who have been identified as “potentially” not citizens, “from any official information source,” including DHS and the DMV.
- Documents related to removing voters from the rolls based on citizenship.
- Documents related to “individuals who claimed to be non-U.S. citizens when attempting to avoid” jury service.³

J.A. 59-60.

³ The Board does not have access to any documents related to jury service. Recently, and after PILF’s requests here, the North Carolina General Assembly passed a bill that would have allowed the Board to access jury responses of the kind sought by PILF, but the bill was vetoed. *See* Governor Roy Cooper Objections and Veto Message, S. Bill 250 (Nov. 6, 2019), <https://webservices.ncleg.gov/ViewBillDocument/2019/6866/o/S250-BD-NBC-8368>.

In addition, PILF described the types of records it expected to receive on individual voters. It demanded:

- Completed voter-registration applications and voter profiles;
- Communications from voters, including “from legal counsel or claimed relatives;”
- Documents from federal agencies, including DHS and USCIS;
- Documents relating to “pending immigration matters”;
- Responses by voters to requests for proof of citizenship—responses that include personal documents like passports and birth certificates.

J.A. 59-61.

In its demands, PILF cited a federal statute, the NVRA. Congress enacted the NVRA to “promote the exercise” of the right to vote and to overcome “discriminatory and unfair” voter-registration procedures. 52 U.S.C. § 20501(a)(2)-(3). For example, “many States continue[d] to penalize non-voters by removing their names from the voter-registration rolls merely because they have failed to cast a ballot in a recent election.” S. Rep. No. 103-6, 17 (1993). Congress found that these “purge systems,” in addition to being “highly inefficient and costly,” had “a long history” of being used to “violate

the basic rights of citizens,” particularly “minority communities.” *Id.* at 18. Thus, Congress designed the NVRA both to encourage voter registration, and “to ensure that once a citizen is registered to vote, he or she should remain on the voting rolls so long as he or she remains eligible to vote.” *Id.* at 17.

To accomplish these goals, the NVRA requires states to provide at least three different ways for voters to register: when they apply for a driver’s license, by mail, and at certain public agencies. 52 U.S.C. §§ 20503-06.

Section 8 of the NVRA limits the ability of states to purge voters from the voting rolls. *Id.* § 20507. In particular, section 8 bars states from removing voters from the rolls, except: (1) at the voter’s request, (2) if the voter is ineligible under state law “by reason of criminal conviction or mental incapacity,” (3) “death,” or (4) “a change in residence” that makes them ineligible to vote in that jurisdiction. *Id.* § 20507(a)(3)-(4).

Section 8 goes on to require states to conduct a “general program” that makes “a reasonable effort” to remove voters based on these grounds. *Id.* § 20507(a)(4). Any state “program” or “activity” to remove voters from the rolls must be “uniform, nondiscriminatory, and in compliance with the Voting Rights Act.” *Id.* § 20507(b)(1). The law also provides detailed

instructions for how states can comply with the law. *See id.* §§ 20507(b)-(g). For example, the law describes an address-verification process by which states “may meet” section 8’s requirements. *Id.* § 20507(c). For states that decline this safe harbor, the law imposes detailed limits on the procedures that they can use to remove voters from the rolls. *Id.* § 20507(d).

Finally, to ensure that the public can enforce section 8’s limits on voter purges, subsection (i) provides for states to disclose “all records” concerning the “implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters.” *Id.* § 20507(i)(1).

C. The Board Complied with PILF’s Requests to the Extent Allowed by Law.

After carefully considering PILF’s requests, the Board provided PILF with extensive responsive documents both electronically and in person. It also explained how PILF could obtain further records. The Board explained, however, that complying with some of PILF’s requests would violate the law.

The Board provided expansive disclosures to PILF, including the following categories of records:

- Voter-list maintenance records for every registered voter in the State. These records are updated weekly and are freely available to the public. The records identify every individual removed from the voting rolls, the reason for removal, and the date of removal. J.A. 82.
- Voting-history records for every registered voter in the State. J.A. 82.
- The Board's full 2016 audit report. J.A. 25-58. The report includes several categories of responsive information, including:
 - The Board's methods and processes for investigating potential voting by noncitizens. J.A. 33-35.
 - The audit's results, including: (1) the number and nationality of registered voters whom the Board identified as noncitizens, (2) the number of individuals who were erroneously flagged as possible noncitizens by the DMV and SAVE databases, and (3) the number of individuals still being investigated. J.A. 29-30, 58.
 - Copies of redacted correspondence that the Board used to verify voters' citizenship. J.A. 53-57.

The Board explained, however, that it was unable to disclose certain documents: Records that identify “particular individuals” who have been flagged as possible noncitizens. J.A. 83. The Board explained that disclosing this information would violate a number of the Board’s legal obligations.

For example, the Board explained that fully complying with PILF’s request would require the Board to disclose information that it received from confidential government databases. Information in those databases is protected against disclosure by multiple federal privacy laws. Disclosure would also violate the Board’s agreement with the federal government under the SAVE Program. J.A. 83.

The Board further explained that it was “continu[ing] to provide records sought by federal law enforcement.” J.A. 83. The Board provided PILF with copies of memoranda regarding subpoenas from the U.S. Attorney’s office. *See* J.A. 234-37. The Board stated that it could not “presently disclose the identity of any prior or current registrant that may be subject to review by federal law enforcement.” J.A. 83.⁴

⁴ Due to ongoing sealed proceedings, *see, e.g., In Re Sealed Matter*, No. [SEALED], Doc. [Sealed] (E.D.N.C. Dec. 12, 2019), the Board filed below certain documents *ex parte* and under seal. PILF seeks *in camera* review of these sealed proceedings and materials. Appellant’s Br. 48. The Board would also invite the Court to conduct *in camera* review of the sealed

D. PILF Filed This Lawsuit Against the Board.

Unsatisfied by the Board's extensive disclosures, PILF filed this lawsuit. PILF has alleged that the Board violated section 8(i) of the NVRA by not publicly releasing the identities and personal records of individuals being investigated for possibly registering to vote as noncitizens. *See* J.A. 20.

The Board moved to dismiss. The Board argued that the NVRA does not require disclosure here because the records PILF seeks are protected by federal privacy laws, including privacy protections in the U.S. Constitution. J.A. 294-302. Further, the Board explained that the records could not be disclosed because they relate to an ongoing law-enforcement investigation. No. 5:19-cv-00248-BO, Doc. 21, at 1, 26-28; *see also* J.A. 98-99.

The district court granted the Board's motion to dismiss. The court observed that "being identified as an individual who is registered to vote but who may not be a United States citizen raises the specter of immigration violations and criminal activity." J.A. 300 (citing 18 U.S.C. § 611). Thus, the

filings. As these filings show, the Board was required to submit the filings under seal. The Court will further see that, for the reasons cited in the Board's response letter to PILF, the Board cannot comply with PILF's requests in full. J.A. 83. The Board would welcome the opportunity to provide sealed supplemental briefing on this issue, if requested by the Court.

court held that the requested information is plainly “sensitive and vulnerable to abuse.” J.A. 300.

Further, the court observed that PILF’s requests covered not only voter-registration records, but also documents used to verify individuals’ citizenship status. These documents include copies of birth certificates and passports—documents which may be used to perpetrate identity theft. The court held that these sensitive documents were also not subject to public disclosure. J.A. 300.

More broadly, the district court concluded that, “while Congress was concerned with transparency when enacting the NVRA, it was unwilling to completely override individual privacy in areas which may result in either stigma or harassment.” J.A. 300. The court thus concluded that the NVRA does not override other federal statutes, such as the Privacy Act and the Drivers Privacy Protection Act, that protect personal privacy.

This appeal followed.

SUMMARY OF THE ARGUMENT

The district court correctly held that PILF failed to state a claim for relief under the NVRA.

As the district court recognized, PILF's requests ask the Board to identify individuals based on confidential information that the Board obtained from other government agencies. PILF's requests also demand that the Board disclose personally sensitive documents, such as birth certificates and passports.

PILF argues that it is entitled to unlimited disclosure of these records under the NVRA. However, courts may not assume that Congress intended to authorize the disclosure of highly personal information without "clear" and "explicit" statutory language to that effect. *Maracich v. Spears*, 570 U.S. 48, 58 (2013).

Applying this standard, there are several reasons why PILF's arguments fail.

First, the NVRA does not clearly or explicitly require disclosure of the withheld documents. The NVRA is a government-transparency statute, not a tool for targeting individual voters with intrusive demands for personal information. Allowing the statute to be misused in this way would

undermine the NVRA's core purpose by discouraging eligible citizens from registering to vote.

Second, the withheld documents are protected from disclosure under multiple federal privacy laws. The documents contain personal information from motor vehicle records—a category of information that the Driver Privacy Protection Act protects from public disclosure. Additionally, the Privacy Act bars the Board from releasing personal records and other confidential information that it obtains from the federal government. Reading these statutes together with the NVRA confirms that the Board is not required to disclose the requested information.

Third, requiring the Board to disclose sensitive voter information would raise serious doubts about the NVRA's constitutionality. Government disclosures of individuals' personal information may violate their constitutional right to informational privacy. *See Whalen v. Roe*, 429 U.S. 589, 599-600 (1977). This privacy intrusion is particularly dangerous here, because it selectively burdens fundamental voting rights of a protected class. At minimum, the doctrine of constitutional avoidance points toward interpreting the NVRA to avoid these serious constitutional problems.

The Board requests that this Court affirm the judgment below.

ARGUMENT

I. The District Court Correctly Held That The NVRA Does Not Require The Board To Disclose The Withheld Documents.

A. Courts Apply a Strong Presumption that Congress Did Not Intend to Compromise Individual Privacy.

PILF claims that section 8(i) of the NVRA requires the unlimited, bulk disclosure of highly sensitive personal information to the general public—no questions asked. Under Supreme Court precedent, however, courts must presume that Congress would not intend to compromise individual privacy in this way. *Maracich*, 570 U.S. at 64. To overcome that presumption, PILF must show that Congress gave “clear and explicit” instructions to invade individual privacy rights. *Id.* PILF has not met that burden here.

PILF contends that section 8(i) requires disclosure of all records related to voter-registration activities, no matter how sensitive those records may be. PILF relies on this Court’s decision in *Project Vote v. Long*, which held that section 8(i) allows disclosure of completed voter-registration applications. 682 F.3d 331, 340 (4th Cir. 2012). PILF argues that, because section 8(i) requires disclosure of certain voter records, then the statute applies to *all* such records, even those that unduly invade privacy rights.

Project Vote does not support PILF's one-size-fits-all approach. Rather, *Project Vote* confirms that certain categories of highly sensitive information cannot be disclosed under section 8(i). *Id.* at 339. As the Court recognized, certain personal information is so "uniquely sensitive and vulnerable to abuse" that public disclosure of that information would "create[] an intolerable burden" on voting rights. *Id.* (quoting *Greidinger v. Davis*, 998 F.2d 1344, 1355 (4th Cir. 1993)). Thus, the Court upheld the district court's redaction of social security numbers from voter applications, even though section 8(i) does not include any exception for that information. *Id.*

Since *Project Vote*, the Supreme Court has instructed courts to be even more attentive to privacy interests when they interpret federal statutes. In *Maracich*, the Court interpreted a section of the Driver Privacy Protection Act that allowed for disclosure of personal records "in connection with" litigation. 570 U.S. at 58. These personal records included identifying information, photographs, social security numbers, and medical and disability information. *Id.* at 57.

The Court acknowledged that the statute's disclosure provision, when interpreted to its "broadest reach," seemed to require disclosure of wide

swaths of personal information. *Id.* at 59. However, the Court declined to interpret the provision in isolation, explaining that the provision's broad terms "provide[] little guidance without a limiting principle consistent with the structure of the statute and its other provisions." *Id.* at 60.

The Court found such a limiting principle in Congress's intent to protect personal privacy. *Id.* at 60-61. Disclosure of highly personal information "is so substantial an intrusion on privacy," the Court explained, that "it must not be assumed, without language more clear and explicit, that Congress" intended that result. *Id.* at 64.

The Supreme Court's guidance in *Maracich* applies here. Like in *Maracich*, the records PILF seeks are highly sensitive and private. They include confidential data from government databases and personal documents, such as passports and birth certificates. Disclosing such records would invade voters' privacy and pose the same risks of identity theft that this Court has cited to allow nondisclosure of social security numbers. *See Greidinger*, 988 F.2d at 1353-54; accord *True the Vote v. Hosemann*, 43 F. Supp. 3d 693, 738 (S.D. Miss. 2014) (declining to order disclosure of several categories of documents under section 8(i), because identity theft is an

“ever-growing concern” in the age of big data that is “fueled by disclosure” of personal information).⁵

Moreover, information that a voter *may potentially* be a noncitizen is highly stigmatizing, in part because it implicates criminal activity. *Stern v. FBI*, 737 F.2d 84, 91-92 (D.C. Cir. 1984) (“individuals have a strong interest in not being associated unwarrantedly with alleged criminal activity”). Disclosing that information risks “publicly brand[ing]” the identified individuals as criminals—a branding that, for most voters flagged by the Board, would be completely baseless. *United States v. Briggs*, 514 F.2d 794, 803 (5th Cir. 1975). By any measure, being falsely and publicly branded as a criminal is a privacy invasion that equals, if not exceeds, that associated with identity theft. *See infra*, at 64-70.

Given these sensitivities, PILF bears a heavy burden to show that Congress clearly and explicitly required disclosure of the withheld records. As shown below, PILF fails to meet that burden here.

⁵ See, e.g., *Identity Theft*, FBI, <https://www.fbi.gov/investigate/white-collar-crime/identity-theft> (last visited Feb. 11, 2020) (noting that birth dates, addresses, telephone numbers, birth certificates, and passport numbers are used to commit identity theft).

B. PILF Cannot Show that the NVRA Clearly Requires the Board to Disclose the Withheld Documents.

The NVRA does not “clear[ly] and explicit[ly]” require disclosure of the withheld documents. *Maracich*, 570 U.S. at 64. This is true for three reasons.

First, the NVRA’s plain text does not mention disclosure of the type of records here. PILF’s limitless interpretation runs contrary to the teachings of the Supreme Court and this Court, which have consistently upheld privacy interests against general disclosure provisions like that found in the NVRA.

Second, the structure of the NVRA, as a whole, shows a focus on transparency in government *programs* related to voter registration—not in publicly singling out individual voters as potential noncitizens.

Third, requiring disclosure of the withheld documents would chill voter registration and participation, contrary to the NVRA’s central purpose.

i. The text of the NVRA does not require disclosure of personally sensitive information.

The plain text of the NVRA does not require unlimited disclosure of voters’ personal information.

To argue the contrary, PILF relies on section 8(i) of the NVRA. That provision provides that states generally “shall make available for public

inspection . . . all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters.” 52 U.S.C. § 20507(i)(1).

PILF argues that section 8(i)(1)’s use of the word “all” requires unlimited disclosure of any and all documents even tangentially related to voter registration, such as law-enforcement investigations into possible noncitizen voters. Appellant’s Br. 14-16.

The Supreme Court has cautioned, however, against giving undue weight to these kinds of “broad” and “indeterminate” statutory terms. *Mellouli v. Lynch*, 135 S. Ct. 1980, 1990 (2015). Because such words, “extended to the furthest stretch of their indeterminacy, stop nowhere,” *id.*, the Supreme Court has cautioned that they should not be read literally or “in isolation, and without reference to the structure and purpose” of a statute. *Maracich*, 570 U.S. at 59. For example, in *Maracich*, the Supreme Court declined to read the statutory term “any” in the DPPA’s disclosure provision “in literal terms.” *Id.* As the Court explained, such a literalist interpretation would have “no limits” and allow unbridled disclosure of individuals’ personal information. *Id.*

The same principle applies here. When read in context, the word “all” in section 8(i) “tugs in favor of a narrower reading.” *Mellouli*, 135 S. Ct. at 1990 (quoting *Yates v. United States*, 135 S. Ct. 1074, 1083 (2015)). This conclusion is confirmed by several features of section 8(i).

For example, section 8(i) provides for disclosure of records “concerning the *implementation*” of government “programs and activities” to maintain accurate voter rolls. 52 U.S.C. § 20507(i)(1). This disclosure requirement, to the extent it covers records about individual voters, is limited to records that “implement[]” such “programs and activities.” As this Court has already held, it does not extend to literally *all* information about individual voters. *Project Vote*, 682 F.3d at 339.

Indeed, section 8(i) only mentions disclosing records about individual voters for one specific program—an address-verification program not at issue here. Specifically, section 8(i)(2) requires states to disclose “lists of the names and addresses” of individuals who were sent address-verification notices under another section of the NVRA. 52 U.S.C. § 20507(i)(2). That other section requires states to notify voters before removing them from the rolls based on an address change. *Id.* § 20507(d). Thus, section 8 requires disclosure of this particular information to ensure that states are not

improperly purging voters based on address changes. *See* S. Rep. No. 103-6, at 17-18.

This pattern is meaningful here. By specifically mentioning disclosure of only address-verification records, Congress has conveyed that *other* kinds of records on individual voters may not be subject to the disclosure requirement. *Cf. Maracich*, 570 U.S. at 59.

The only other time that section 8(i) mentions individual voter records is to *protect* personal information from disclosure. Specifically, Congress excepted two categories of information from disclosure: (1) the reason for a declination to register to vote, and (2) the identity of an agency through which an individual registers to vote. 52 U.S.C. § 20507(i)(1). Congress enacted these exceptions because they “involve matters of personal privacy.” S. Rep. No. 103-6, at 24. For example, an individual may not want to reveal that she is ineligible to vote due to mental incompetence, or that she registered to vote at a public-assistance agency. *Id.*

PILF contends that these are the *only* exceptions to public disclosure under section 8(i). Appellant’s Br. 22-23. Of course, this Court has already held the opposite: any records that are “uniquely sensitive and vulnerable to abuse” are not subject to disclosure under the NVRA. *Project Vote*, 682 F.3d

at 339. Moreover, as courts have held, it is “reasonable” to conclude that Congress declined to mention other exclusions that apply, because those categories of information are already protected against disclosure by other federal laws. *Tex. Democratic Party v. Bettencourt*, No. H-08-3332, 2009 U.S. Dist. LEXIS 133441, at *20 (S.D. Tex. July 16, 2009). In context, therefore, section 8(i)’s exemptions *supplement* (rather than override) existing privacy protections. *See infra*, at 38-55.

As the above analysis shows, the NVRA’s text does not clearly or explicitly require disclosure of the withheld records here.

ii. The structure of the NVRA shows that Congress was focused on government transparency, not exposing voters’ private information.

PILF’s arguments fare no better when considered against the NVRA’s structure. PILF’s interpretation would convert a government-transparency statute into a tool for exposing voters’ highly sensitive personal information. The NVRA’s structure shows that Congress did not intend that result.

It is a “fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme.” *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2002). Moreover, “identical words used in different parts of the

same act are intended to have the same meaning.” *Gustafson v. Alloyd Co.*, 513 U.S. 561, 570 (1995).

The structure of the NVRA reveals that it is a statute focused on bringing transparency to the activities of governments—not individuals.

The NVRA requires states to establish at least three ways for voters to register to vote. Section 5 of the NVRA, known as the motor-voter law, requires states to allow voter registration when they apply for a driver’s license. 52 U.S.C. § 20504. Section 6 establishes registration by mail. *Id.* § 20505. Section 7 covers in-person registration at public agencies. *Id.* § 20506.

At the same time that it expanded voter registration, Congress took steps to protect individual privacy. Under the NVRA, states may collect “only the minimum amount of information necessary” to assess voter eligibility, prevent duplicate applications, and administer the voter-registration process. *Id.* §§ 20504(2)(A), 20508(b)(1). States must also keep certain voter-applicant information confidential. *Id.* § 20508(b)(4).

Section 8 of the NVRA—the section at issue here—regulates programs for voter registration. *Id.* § 20507. For example, states must establish a “general program that makes a reasonable effort” to remove voters who die

or move outside the jurisdiction. *Id.* § 20507(a)(4). This section does not mention, let alone require, any systemic program for investigating the citizenship status of registered voters.

Section 8 also provides safeguards to prevent states from wrongly removing eligible voters from the rolls. For example, states must notify voters and give them a chance to respond before removal. *Id.* § 20507(d).

Finally, section 8(i) requires states to disclose records concerning the implementation of these voter-related “programs and activities.” *Id.* § 20507(i)(1). This subsection uses the same words—“programs” and “activities”—that are used throughout section 8 to describe the kinds of procedures allowed by the NRVA to remove voters from the rolls. *See, e.g., id.* § 20507(a)(4).

As this analysis shows, section 8(i) is aimed at government programs, not individuals. The “central purpose” of these kinds of government-transparency statutes “is to ensure that the *Government’s* activities be opened to the sharp eye of public scrutiny, not that information about *private citizens* that happens to be in the warehouse of the Government be so disclosed.” *U.S. Dep’t of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 775 (1989). Thus, courts interpret government-transparency

statutes not to require disclosure of private information simply because it happens to be held by a government entity. *See id.*; *see also Trentadue v. Integrity Committee*, 501 F.3d 1215, 1234 (10th Cir. 2007); *Stern*, 737 F.2d at 91-92.

Under these principles, the NVRA does not require disclosure of the withheld documents. Even assuming there were “some public interest” in releasing records of voters identified as potentially noncitizens, disclosing this highly sensitive information “falls outside the ambit of the public interest” that the NVRA was enacted to serve. *Reporters Committee*, 489 U.S. at 775.

iii. Disclosing the withheld information would undermine the NVRA’s purpose.

Disclosing the withheld records is also not warranted here, because disclosure would undermine the NVRA’s fundamental purposes. Those purposes are to enhance voter registration and to prevent eligible voters from being removed from the voting rolls.

“The meaning of a statutory provision is not to be determined in isolation; ‘we look not only to the particular statutory language, but to the statute as a whole and to its object and policy.’” *Gaines Motor Lines, Inc. v.*

Klaussner Furniture Indus., Inc., 734 F.3d 296, 303 (4th Cir. 2013) (quoting *Crandon v. United States*, 494 U.S. 152, 158 (1990)).

Here, the fundamental purpose of the NVRA is to increase voting and to eradicate discrimination in voting-registration procedures. In enacting the NVRA, Congress found that the right to vote is “fundamental,” that states have a duty “to promote the exercise of that the right,” and that “discriminatory and unfair registration laws” directly harm voter participation, especially by racial minorities. 52 U.S.C. § 20501(a).

Consonant with these findings, Congress enacted the NVRA to remove obstacles to voter registration. *See id.* § 20501(b). The NVRA’s legislative history is suffused with Congress’s emphasis on improving voter turnout and making registration easier. *See* S. Rep. No. 103-6, at 1-4 (discussing the nation’s history of poor voter turnout and testimony describing how registration procedures deter voters); H. Rep. No. 103-9, at 3 (1993) (“The unfinished business of registration reform is to reduce these obstacles [to registration] to the absolute minimum while maintaining the integrity of the electoral process.”).

While Congress was “mindful of the need to keep accurate and current voter rolls,” its overriding concern was that voter list-maintenance programs

“can be abused and may result in the elimination of eligible voters from the rolls.” S. Rep. No. 103-6, at 32. For this reason, section 8 of the NVRA includes numerous safeguards to prevent states from improperly removing eligible voters from the rolls. *See* 52 U.S.C. §§ 20507(a)-(e).

Requiring disclosure of voters’ sensitive personal information would undermine these fundamental purposes. Here, PILF requests confidential information obtained from outdated and imperfect government databases, as well as voters’ sensitive personal records. If these requests were granted, the affected voters—the majority of whom are eligible citizens—would be publicly branded as possible felons. *See Briggs*, 514 F.2d at 803.

The disclosures would therefore have a chilling effect on the willingness of many Americans to register to vote at all. As courts have recognized, if Americans knew that registering to vote could result in the bulk disclosure of their personal information, they would be discouraged from exercising their fundamental right to vote. *True the Vote*, 43 F. Supp. 3d at 739; *Project Vote v. Long*, 752 F. Supp. 2d 697, 711-12 (E.D. Va 2010); *Texas Democratic Party*, 2009 U.S. Dist. LEXIS 133441, at *27. This danger is heightened here, because the requested disclosures disproportionately target a protected class: voters who are naturalized citizens. *See infra*, at 69-71.

Indeed, in *Greidinger*, this Court agreed that disclosing voters' personal information burdens voting rights. 988 F.2d at 1355. In *Project Vote*, the Court allowed disclosure of voters' sensitive information (like their history of felony convictions), but it did so only because that information was "already a matter of public record." 682 F.3d at 339 n.*. Here, by contrast, the Board has fully disclosed all information within the scope of PILF's requests that is publicly available. The withheld documents concern information that, unless ordered disclosed here, is strictly private. *See supra*, at 12-13.

PILF dismisses the burden of disclosure on voting rights by observing that noncitizens do not have the right to vote. Appellant's Br. 32. But as PILF knows, the vast majority of voters who are investigated as possible noncitizens turn out to be citizens who are eligible to vote. J.A. 209.

PILF also fails to explain how disclosing the withheld documents would further the NVRA's purposes. PILF cannot identify any reason to believe that the Board has not properly discharged its duty to maintain the integrity of the electoral process. Thus, the Board is entitled to a "presumption of legitimacy" in its law-enforcement activities. *National Archives and Records Admin. v. Favish*, 541 U.S. 157, 174 (2004).

These circumstances contrast starkly with *Project Vote*, which involved a voting-rights group's effort to combat suspected voter suppression. 682 F.3d at 333. In that case, Project Vote requested certain voter-registration records because it had reason to believe that a state had unlawfully rejected voter applications from students at a historically black university. *Id.* As the Court held, the state was required to disclose registration forms of voters whose applications may have been rejected for discriminatory reasons. *Id.* at 334. That order aligned with the NVRA's purpose: to ensure that states do not administer "purge systems" to disproportionately remove members of "minority communities" from the voting rolls. S. Rep. 103-6, at 18.

Thus, in *Project Vote*, this Court ordered disclosure of records to *protect* the voting rights of minority communities. In that case, the affected individuals had a strong interest in disclosure of their private information, to safeguard their voting rights. Here, by contrast, disclosure would burden not only privacy rights, but voting rights as well.⁶

⁶ As explained below, the Privacy Act expressly bars disclosure of the withheld documents. *See supra*, at 45-50. The applicability of the Privacy Act further distinguishes this case from *Project Vote*. That case involved the disclosure of purely state records—records that are not protected by the Privacy Act because they lack any federal source. 682 F.3d at 333. Thus, the parties in *Project Vote* did not raise, and this Court did not consider, the Privacy Act. *See id.*

Similarly, while PILF relies on *Arcia v. Florida Secretary of State*, that case involved voters' and voting rights groups' efforts to prevent a state from unlawfully purging citizens who had been wrongly flagged as noncitizens. 772 F.3d 1335, 1339-40 (11th Cir. 2014). The case did not address whether the NVRA required *public disclosure* of information concerning the voters flagged as noncitizens. Instead, the plaintiffs alleged that Florida was systemically purging the voter rolls too close to an election, in violation of a separate provision of the NVRA. *Id.*

* * *

In sum, PILF's overbroad reading of section 8(i) is not supported by the NVRA's text, structure, or purpose. Thus, the district court was right to dismiss PILF's claim that the NVRA requires the Board disclose the withheld materials.

II. The Withheld Records Are Protected From Disclosure By Federal Privacy Laws.

As shown above, the NVRA does not require the withheld documents to be disclosed. But beyond that, those documents are expressly *protected* from disclosure under federal privacy laws, including the Driver Privacy Protection Act and the Privacy Act.

The withheld records contain protected personal information from at least three sources: (1) personal DMV records, (2) federal databases operated by the SAVE program, and (3) the Board's investigation of individual voters. As shown below, the Board cannot turn over any of these records without violating federal privacy laws.

A. The NVRA and Federal Privacy Laws Must Be Read Together as an Inclusive Whole.

It is a cardinal rule of statutory interpretation that “courts not interpret statutes in isolation, but in the context of the *corpus juris* of which they are a part.” *Branch v. Smith*, 538 U.S. 254, 281 (2003). Thus, absent a contrary indication, “the Court should interpret [multiple] statutes *in pari materia*, that is, in a consistent manner.” *United States v. Banker*, 876 F.3d 530, 538 (4th Cir. 2017).

This canon applies with special force when statutes “address[] the same subject matter,” *Wachovia Bank v. Schmidt*, 546 U.S. 303, 316 (2006), or “function as parts of a greater whole,” *Elec. Welfare Tr. Fund v. United States*, 907 F.3d 165, 168 (4th Cir. 2018). Because both the NVRA and federal privacy laws cover the potential disclosure of private information, these statutes must be viewed together, “as if they were one law.” *Wachovia Bank*, 546 U.S.

at 316. Taking this interpretive approach here confirms that the Board was right to refrain from disclosing to PILF sensitive information covered by the privacy statutes.

B. The Driver Privacy Protection Act Bars Disclosure of the Withheld Documents.

The Board's first step in verifying voter citizenship was to compare the voting rolls against DMV records. Those records include codes that purport to reflect a person's noncitizen status. They also include other personally identifying information that the Board used in its investigations, such as alien identification numbers.

This personal information is protected from disclosure by the Driver Privacy Protection Act. Congress passed the DPPA to address privacy concerns raised by public access to DMV records, including the ability of criminals to use those records to obtain personal information on their potential victims. *See Taylor v. Acxiom Corp.*, 612 F.3d 325, 336 (5th Cir. 2010) (describing DPPA's legislative history).

Congress passed the DPPA *just a year* after it passed the NVRA. This timing alone strongly suggests that Congress intended the two statutes to work together. The two statutes overlap substantively as well: the NVRA

allows voters to register to vote when they apply for a driver's license. 52 U.S.C. § 20504. The DPPA guarantees that information supplied on drivers-license applications remains private. 18 U.S.C. § 2721(a). Given this overlap, Congress presumably intended for the DPPA to guarantee the privacy of driver records, even though it had previously required those agencies to engage in voter-registration activities that could be subject to public disclosure under the NVRA. *Lake v. Neal*, 585 F.3d 1059, 1061 (7th Cir. 2009) (explaining the application of both statutes to motor vehicle agencies); see *Goodyear Atomic Corp. v. Miller*, 486 U.S. 174, 185 (1988) (courts “presume that Congress is knowledgeable about existing law pertinent to the legislation it enacts”).

Specifically, the DPPA prohibits a state DMV and its representatives from disclosing “personal information . . . obtained by the department in connection with a motor vehicle record.” 18 U.S.C. § 2721(a). “Personal information” is defined as any “information that identifies an individual, including an individual’s photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information.” *Id.* § 2725(3).

Under this definition, the withheld records cannot be disclosed because they contain “personal information” that is obtained “in connection with a motor vehicle record.” 18 U.S.C. § 2721(a); *Pub. Interest Legal Found. v. Boockvar*, No. 1:19-CV-622, 2019 WL 6828620, at *8 (M.D. Pa. Dec. 13, 2019) (holding that the DPPA prevents state election boards from re-disclosing personal information obtained from driver records). Moreover, in the unique circumstances of PILF’s requests, the withheld records cannot be released in redacted form. Releasing these records in any form would risk identifying voters who were tagged as noncitizens based on DMV data. That identification itself would disclose “personal information” gleaned from DMV records, and would thus violate the DPPA.

PILF’s arguments that the DPPA does not protect these records fall short.

Initially, PILF argues that the DPPA does not apply because “the Foundation has not asked to inspect motor vehicle records.” Appellant’s Br. 41. However, the DPPA protects far more than just motor vehicle records themselves. Rather, the law protects all “personal information” that is obtained by the DMV “*in connection with* a motor vehicle record.” 18 U.S.C. § 2725(1) (emphasis added). Courts have applied this definition to hold that

personal information comes from a motor vehicle record when it derives from DMV sources and pertains to a permit, license, title, or identification issued by the DMV. *See Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 949 (7th Cir. 2015); *Lake*, 585 F.3d at 1061; *Siegler v. Best Buy Co.*, 519 F. App'x 604, 605 (11th Cir. 2013). Here, the information the Board collected from the DMV included personal information for drivers whose “license contains a restriction code related to their non-citizen status.” J.A. 208. Thus, the withheld records are protected by the DPPA because they include personal information derived from individual driver’s license records.

PILF also claims that citizenship status is not “personal information” because it does not identify an individual. Appellant’s Br. 42. This argument fails. To begin with, PILF’s requests plainly seek information that identifies particular individuals. *See* J.A. 59-61, 83, 208-09.

More broadly, the argument overlooks that the DPPA includes a broad, open-ended definition of “personal information.” 18 U.S.C. § 2725(3). By using the word “including” to introduce the examples in the definition, Congress intended to show that those examples are merely illustrative, not exhaustive. *See Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 578 (1994) (the term “including” indicates the “illustrative and not limitative function of

the examples given”). Thus, the DPPA protects *any* information that can be used identify to a person, including citizenship status, alien identification numbers, and other personal information used to match a driver to a voter record. *See United States v. Hastie*, 854 F.3d 1298, 1304 (11th Cir. 2017); *Dahlstrom*, 777 F.3d at 942.

Next, PILF argues that the DPPA does not apply to elections boards, but only motor vehicle agencies. Appellant’s Br. 44. However, by its terms, the DPPA’s nondisclosure requirements apply to *any* agency that lawfully receives information from a DMV. *See* 18 U.S.C. § 2721(c) (prohibiting agencies from re-disclosing driver license records for non-permitted uses). Thus, the DPPA applies to the Board.

Similarly, PILF argues that even if the Board cannot disclose personal information received from the DMV, it may disclose any *derivative* records based on that information. Appellant’s Br. 46. PILF cannot cite any court that has embraced this distinction—and it is easy to see why. PILF’s derivative-records theory would allow states to effectively nullify the DPPA’s protections. If the DPPA protects personal information when the DMV releases it to the Board, then that information must remain protected when the Board uses it. Thus, as courts have held, “to the extent [records]

implicate protected personal information contained in DMV records, they are shielded by the DPPA.” *Boockvar*, 2019 WL 6828620, at *7.

Finally, PILF argues that it should be considered a state actor—a “private attorney general”—that is entitled to receive DMV information on equal terms as a government agency. Appellant’s Br. 45-46. That argument lacks any basis in the law. The DPPA contains several carefully crafted exceptions allowing disclosure, none of which allow private groups to anoint themselves as quasi-government actors in order to obtain private confidential information. See 18 U.S.C. § 2721(b).

In sum, the DPPA bars disclosure of any information that contains individual voters’ personal information derived from DMV records.

C. The Privacy Act Also Bars Disclosure of the Withheld Documents.

The Privacy Act adds a second layer of statutory protection against disclosure of the withheld documents.

Congress passed the Privacy Act “out of concern over the ‘impact of computer data banks on individual privacy.’” *Reporters Committee*, 489 U.S. at 766 (quoting H.R. Rep. No. 93-1416, at 7 (1974)). To address this concern, the Act gives individuals broad privacy rights over private or personal

information that is held by the federal government. The Act applies whenever a party seeks to force the government to disclose private information. And so long as the NVRA and federal privacy laws are “capable of co-existence,” courts have a “duty . . . to regard each as effective.” *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1018 (1984).

Here, the Privacy Act limits disclosure of the withheld records in two ways.

First, the Act bars agencies from publicly disclosing personal information that is held in federal databases. Specifically, the Act prohibits federal agencies from “disclos[ing] any record which is contained in a system of records” to any person or entity, other than with the consent of the affected individual. 5 U.S.C. § 552a(b). The Act defines a “record” as “any item, collection, or grouping of information about an individual” that is maintained by an agency and contains identifying information. *Id.* § 552a(a)(4). Although the Privacy Act does not regulate states directly, the Act’s disclosure bar applies to any entity, such as the Board, that accesses federal records to carry out government functions. *Id.* § 552a(m)(1).

When investigating potential noncitizen voters, the Board accessed immigration records and databases maintained by the federal government.

Those documents are “records” that are maintained within a “system of records” protected by the Act. *See id.* § 552a(a)(4); *see also* Dep’t of Homeland Sec., Privacy Impact Assessment for the SAVE Program 2 (2011), https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_save.pdf. Thus, the Privacy Act bars the Board from disclosing any information from the SAVE Program without the affected individual’s consent. *See* 5 U.S.C. § 552a(b).

Second, the Privacy Act bars the Board from disclosing information it receives from the SAVE Program for another reason. The Act strictly limits an agency’s use of automated programs to “match” individual records with other government databases. *See id.* § 552a(o). The Act requires agencies that use such matching programs to enter into an agreement that provides procedures for (1) ensuring the security of shared records, and (2) protecting against the re-disclosure of shared records. *Id.* §§ 552a(o)(G), (H).

The SAVE Program is a computer-matching program within the meaning of the Privacy Act. SAVE Program Guide at 1. Therefore, agencies that use the SAVE Program must enter an agreement with the federal government that safeguards personally identifying information, as the Board did here. *Id.*; J.A. 190-99.

PILF is wrong to argue that the NVRA overrides the SAVE agreement and the Privacy Act protections on which it relies. Appellant's Br. 38-39. As the agreement shows, the Board was granted access to the SAVE Program based on the explicit condition that the Board would comply with the Privacy Act. J.A. 197. Construing the NVRA to nullify this condition—and to require unlimited public disclosure of information from confidential federal government databases—would destroy the legal basis on which the Board obtained the requested information in the first place. More broadly, it would discourage the federal government from allowing states to access the SAVE Program databases. Because DMV records showing noncitizen status are inaccurate over 97% of the time, this result would make it far more difficult for states to investigate whether noncitizens had registered to vote. J.A. 209.

PILF argues that disclosure is nonetheless required because the SAVE agreement states that it does not “limit or affect the duties, responsibilities, and rights” of the Board under the NVRA. Appellant's Br. 39-40 (citing J.A. 198). However, this generic provision does not purport to allow the Board to disclose personal information that is protected against disclosure by other federal laws like the Privacy Act. Rather, the provision ensures that the

Board does not abuse the SAVE Program for discriminatory purposes. For instance, the agreement requires the Board to “[c]omply with federal laws prohibiting discrimination against registrants and discriminatory use of the SAVE program.” J.A. 194. At the same time, the agreement repeatedly affirms “that the information . . . receive[d] from DHS-USCIS is governed by the Privacy Act.” J.A. 197. Thus, the SAVE agreement confirms that information the State obtains from the program remains protected by the Privacy Act.

Finally, PILF argues that applying the Privacy Act here would go too far, because it would extend to voter addresses that are obtained through the National Change of Address Program. Appellant’s Br. 40. The NVRA explicitly provides that voter-address information must be disclosed to the public when states seek to remove voters from the rolls based on a change in address. 52 U.S.C. §§ 20507(i)(2). Whether this provision clashes with the Privacy Act is simply not relevant here. Nothing in the NVRA specifically addresses citizenship-related information or any other category of information withheld by the Board.

In sum, the withheld documents fall squarely within the Privacy Act’s protections. Thus, reading the two statutes together, the Privacy Act limits

section 8(i) of the NVRA to bar the government from publicly disclosing private information about particular persons.

D. PILF Cannot Show that Congress Intended the NVRA to Displace All Other Privacy Laws.

Under PILF's interpretation of the NVRA, section 8(i) would override wide swaths of federal and state privacy laws. It would also enable bad actors to use the NVRA to engage in unlimited abuse of private information, including identity theft. PILF has not shown that Congress intended this ancillary statutory provision to have such dramatic results.

PILF does not dispute that, under its interpretation of the NVRA, section 8(i) would override all federal, state, and common-law privacy protections that protect voters' information. In PILF's view, all personal records that happen to overlap in any way with a state's maintenance of voter rolls are subject to unlimited public disclosure. Such an "unrestrained interpretation" would create "a gaping hole in the statutory landscape whereby personal, otherwise protected information would lose its protection once a citizen registered to vote." *Hosemann*, 43 F. Supp. 3d at 735. This result is "simply irresponsible" and contrary to "common sense." *Tex. Democratic Party*, 2009 U.S. Dist. LEXIS 133441, at *25.

As the Supreme Court has held, courts presume that Congress does not fundamentally remake a comprehensive regulatory scheme “in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes.” *Whitman v. American Trucking Ass’n*, 531 U.S. 457, 468 (2001).

Here, however, PILF would interpret a modest disclosure provision, which is designed to further the NVRA’s overriding purpose to promote voter registration, to instead nullify a landscape of federal and state laws that protect individual privacy. These laws include:

- Federal privacy statutes, such as the Privacy Act and the DPPA. *See supra*, at 39-50.
- Information protected by the constitutional right to privacy. *See Whalen*, 429 U.S. at 599-600; *see also infra*, at 56-71.
- Documents that are protected from disclosure under the Freedom of Information Act (FOIA). For example, FOIA exempts law-enforcement records whose disclosure “could reasonably be expected to constitute an unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(7)(C).

- Documents subject to traditional law-enforcement privileges, like grand jury materials. *See United States v. Coughlan*, 842 F.2d 737, 739 (4th Cir. 1988).
- Documents that are sealed pursuant to a court order. *See* Fed. R. Civ. P. 5.2(d); *see also supra*, at 17 n.4.
- Documents that are classified under federal law, such as diplomatic correspondence regarding immigration enforcement. *See* 18 C.F.R. § 17.22.
- Information protected from disclosure under the Federal Rules of Civil Procedure, such as records of cases involving immigration benefits. Fed. R. Civ. P. 5.2(c).
- State privacy laws. For example, North Carolina’s Public Records Act protects from disclosure “[r]ecords of criminal investigations conducted by law enforcement agencies,” N.C. Gen. Stat. § 132-1.4(a), which includes the Board, *id.* § 132-1.4(b)(3).
- State common law torts that protect against privacy intrusions, such as claims for private disclosure of public facts. *See, e.g., id.* § 75-66.

Although this Court has never specifically addressed whether the NVRA overrides federal privacy laws, it has consulted these laws to assess the limits on public disclosure required by the NVRA. In striking down a voter-registration law requiring public disclosure of social security numbers, for example, the Court emphasized that this information is protected by the Privacy Act and FOIA. *Greidinger*, 998 F.2d at 1354.

Other courts, moreover, have squarely rejected the result PILF seeks here. These courts recognize that an array of privacy laws limit the scope of information that must be disclosed under section 8(i) of the NVRA. *See, e.g., Texas Democratic Party*, 2009 U.S. Dist. LEXIS 133441, at *21 n.9 (“Plaintiffs do not offer an explanation to resolve the conflict between their position that they are entitled to all of the information and federal law protecting certain information”); *Boockvar*, 2019 WL 6828620, at *8 (courts “presume that Congress knew of the potential interplay” between privacy laws and the NVRA’s disclosure mandate); *Hosemann*, 43 F. Supp. 3d at 735 (“It is hard to imagine that in enacting the NVRA, Congress intended to abrogate all protections provided for by Federal and State laws against the disclosure of private and confidential information.”); *Project Vote v. Kemp*, 208 F. Supp. 3d 1320, 1345 (N.D. Ga. 2016) (“it is illogical [to claim] that in

enacting the NVRA, Congress intended to erode Federal and State law protecting against the disclosure of private, personal information”).

By contrast, the only case that PILF cites to support its position that the NVRA overrides all other privacy laws is a two-page district court order. That order reasons in its entirety: “the DPPA does not apply to the disclosure of the voter information requested by Plaintiff.” Appellant’s Br. 42-43 (citing J.A. 254-55). This sparse reasoning cannot justify the expansive result PILF seeks here.

Even more concerning, PILF’s position here would facilitate the unchecked abuse of personally sensitive information. PILF’s interpretation of section 8(i) would “enable any person or organization, regardless of residency, citizenship, or purpose, to obtain almost all personal information . . . of millions of people through simple written requests.” *Hosemann*, 43 F. Supp. 3d at 738. They could then use the information for nefarious purposes, including identity theft and voter intimidation. Under PILF’s expansive reading of the NVRA, it would be “difficult, if not impossible” for courts to prevent requests by individuals with illicit motives. *Texas Democratic Party*, 2009 U.S. Dist. LEXIS 133441, at *24.

PILF's broad requests to the Board highlight the potential for abuse. For example, PILF seeks highly sensitive documents—such as birth certificates, passports, and certificates of naturalization. The NVRA does not require courts to open the “floodgates” to unlimited disclosure of this kind of confidential personal information. *Id.* at *24.

III. PILF's Expansive Reading Of NVRA Section 8(i) Would Raise Serious Doubts About The Statute's Constitutionality.

As explained above, the best reading of the relevant statutes is that the NVRA does not require disclosure of the information requested by PILF here. But if there were any doubt on that score, this Court should interpret the NVRA to avoid the serious constitutional problems that are created by PILF's expansive reading of that law.

“It is a cardinal principle of statutory interpretation that when an Act of Congress raises a serious doubt as to its constitutionality,” courts must first “ascertain whether a construction of the statute is fairly possible by which the question may be avoided.” *Zadvydas v. Davis*, 533 U.S. 678, 689 (2001). In this situation, when an interpretation of a statute that avoids the constitutional question is “fairly possible,” courts are “obligated” to embrace it. *INS v. St. Cyr*, 533 U.S. 289, 300 (2001).

Here, the doctrine of constitutional avoidance provides yet another reason to affirm the judgment below.

A. The Supreme Court and This Court Have Long Recognized a Constitutional Right to Informational Privacy.

The Constitution protects an individual's right to privacy. This privacy right was first articulated by Justice Brandeis as "the right to be let alone—the most comprehensive of rights and the right most valued by civilized man." *Walls v. City of Petersburg*, 895 F.2d 188, 192 (4th Cir. 1990) (quoting *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

As a comprehensive right, the Supreme Court has applied it in a variety of settings. For example, the Court has extended Fourth Amendment protections against unreasonable searches and seizures to situations where the government violates an individual's "reasonable expectation of privacy." *United States v. Jones*, 132 S. Ct. 945, 950 (2012). The Court has also recognized a privacy interest in "independence in making certain kinds of important decisions." *Whalen*, 429 U.S. at 599-600.

Notably, the Supreme Court and this Court have also recognized a privacy right that protects "the individual interest in avoiding disclosure of

personal matters.” *Walls*, 895 F.2d at 192 (quoting *Whalen*, 429 U.S. at 599); *Taylor v. Best*, 746 F.2d 220, 225 (4th Cir. 1984) (same).

This right to informational privacy bars disclosure of the information that PILF seeks here.

At its core, this right protects against government disclosures of personal information about identified individuals to the public. And as this Court has held, laws mandating public disclosure of private information are subject to the most exacting test known to constitutional law: strict scrutiny. *Walls*, 895 F.2d at 192.

The Supreme Court first addressed the right to informational privacy more than forty years ago, in *Whalen v. Roe*. The case involved a challenge to a New York law that required medical doctors to provide the State with a copy of all prescriptions they issued for certain drugs, as well as the names of the patients to whom they prescribed the drugs. 429 U.S. at 591.

The Court stated that this mandatory-disclosure regime implicated the patients’ “individual interest in avoiding disclosure of personal matters” to the government—an interest that was rooted in “the Fourteenth Amendment’s concept of personal liberty.” *Id.* at 598-99 & n.23.

Because the law burdened constitutional rights, the Court evaluated the privacy claim by applying a balancing test. Specifically, the Court weighed the government's interest in compelling disclosure of the prescribing information against the burden imposed on individual privacy rights.

Applying that test, the Court held that the government's "vital interest in controlling the distribution of dangerous drugs" outweighed the law's minimal intrusion on privacy rights. *Id.* at 598. The Court emphasized that the law's burden on privacy rights was minor, because it only compelled disclosure of private information to the government—not to the general public. Thus, the law did not implicate the core feature of the constitutional right to informational privacy: the "right of an individual not to have his private affairs made public by the government." *Id.* at 599 n.24.

The Court cited several features of the law that made the risk of public disclosure remote. For example, only a few state employees had access to the information. *Id.* at 595. Those employees were required to keep the information confidential—on pain of criminal penalties. *Id.* Further, the records were held in a locked "vault" and were destroyed after five years. *Id.* at 594.

Because of these and other extraordinary security features, the Court held that the New York law “evidence[d] a proper concern with, and protection of, the individual’s interest in privacy.” *Id.* at 605. Thus, the Court held that the law did not “pose a sufficiently grievous threat” to individual privacy rights to violate the Constitution. *Id.* at 600.

Although it upheld the law, the Court pointedly recognized “the threat to privacy implicit in the accumulation of vast amounts of personal information” by the government, “much of which is personal in character and potentially embarrassing or harmful if disclosed.” *Id.* at 605. The Court observed that the constitutional dangers posed by government data collection are limited, because the government’s “right to collect and use such data . . . is typically accompanied by a statutory or regulatory duty to avoid unwarranted disclosures.” *Id.* However, the Court warned that, when such protections are absent, government collection of private information could give rise to serious constitutional concerns. *Id.*; *see also Riley v. California*, 573 U.S. 373, 394-95 (2014) (recognizing heightened privacy concerns when the government accumulates vast amounts of personal data).

Since the landmark *Whalen* case, the Supreme Court has twice reaffirmed that the Constitution protects an individual right to informational

privacy. In both cases, the Court recognized that the Constitution bars the government from disclosing personal information about particular individuals to the public.

For example, in *Nixon v. Administrator of General Services*, the Court applied *Whalen*'s balancing test to reject President Nixon's challenge to a federal statute that allowed government archivists to access his presidential papers. 433 U.S. 425, 465 (1977). The Court held that even the President "has a legitimate expectation of privacy in his personal communications." *Id.* However, the Court concluded that those privacy rights were outweighed by the public's interest in access to official records on the presidency. *Id.*

In weighing the strength of Nixon's privacy interest, the Court emphasized the law's various safeguards against a president's purely private papers being disclosed publicly. Under the challenged statute, Nixon's papers were made available only to a small set of professional archivists who would archive any "Presidential materials," and return to him any "private materials." *Id.* at 462, 458-59.

Similarly, in *NASA v. Nelson*, the Court applied the *Whalen* balancing test to decide a constitutional challenge to a NASA job requirement that employees submit to background-check investigations. 562 U.S. 134 (2011).

Those investigations required the employees to disclose to the government, for example, if they had recently used illegal drugs. *Id.* at 141.

The Court again applied the *Whalen* balancing test to reject the constitutional challenge. When assessing the government's interest, the Court emphasized that courts "must take into account the context in which [the privacy intrusions] arise." *Id.* at 148. Here, "the Government conducts the challenged background checks in its capacity as proprietor and manager of its internal operation"—a context where it has "a much freer hand . . . than it does when it brings its sovereign power on citizens at large." *Id.* The government has a strong interest in conducting employee background checks to ensure "the security of its facilities" and to employ "a competent, reliable workforce." *Id.* at 150.

The Court also held that background investigations only minimally burden privacy rights, because the employees "attack only the Government's *collection* of information"—not its public dissemination. *Id.* at 156. The Court emphasized that the Privacy Act "shielded" plaintiffs' personal information from public disclosure in a variety of ways, such as by "requir[ing] written consent before the Government may disclose records pertaining to any individual." *Id.* The Privacy Act's protections against

public disclosure thus “give forceful recognition” to individual privacy rights—recognition that provides constitutionally adequate “safeguards against public disclosure.” *Id.*

This Court has likewise recognized that the Constitution protects individuals against undue government intrusion into their informational privacy. Indeed, this Court has held that informational privacy claims are subject to strict scrutiny. *Walls*, 895 F.2d at 192.

For example, in *Walls*, this Court held that the Constitution bars the government from forcing its employees to disclose certain kinds of personal information in a background investigation. 895 F.2d at 188-89. As the Court explained, “[p]ersonal, private information in which an individual has a reasonable expectation of confidentiality is protected by one’s constitutional right to privacy.” *Id.* at 192. The Court held that the government’s inquiries were valid only if they were “narrowly drawn” to advance “a compelling governmental interest in disclosure.” *Id.* Under this standard, the Court held that the government could not inquire into personal “details that are not part of the public record concerning a divorce, separation, annulment, or the birth of children.” Those kinds of information “are private and thus protected” by the Constitution. *Id.* at 193.

Importantly, the Court enforced the employees' privacy interests, even though it was unlikely that the plaintiff's private information would ever be disclosed publicly. *Id.* at 194 (noting that the background-check records were "kept in a private filing cabinet that is locked at night"). The Court made clear that many more of the background-check questions would have been invalid if the employees' responses "had been more widely distributed." *Id.*; see *Taylor v. Best*, 746 F.2d 220, 225 (4th Cir. 1984) (holding that the Constitution allows prisons to require inmates to answer certain personal questions during standard intake procedures, but only because the prisoner's answers are "confidential").

In sum, this Court and the Supreme Court have recognized a robust constitutional right to informational privacy. For the government to invade that right, it must show that doing so is (1) narrowly tailored to advance compelling government interests, and (2) that those interests outweigh individual privacy rights. The decisive factor in this analysis is often whether the government has established adequate statutory or other safeguards to prevent private information from being publicly disclosed. Absent such safeguards, even the mere collection of sensitive personal information is constitutionally suspect. That suspicion is significantly elevated when the

government goes beyond merely demanding private information, but also disseminates that information widely to the general public.⁷

B. Disclosing the Private Information Requested by PILF Would Violate the Constitution.

Under the above principles, complying with PILF's requests would collide with constitutional protections for informational privacy. Applying the *Whalen* balancing test here shows that any benefits of disclosure are far outweighed by the burden that disclosure would impose on individual privacy rights.

In this case, PILF asks the government to publicly disclose the identities of individual North Carolinians whom the Board has investigated for potential voter fraud. J.A. 78. It also asks to disclose personal documents that the Board has used to clear the vast majority of those individuals of any wrongdoing—documents such as citizenship papers, passports, birth certificates, and social security cards. J.A. 59-68.

⁷ Federal appellate courts across the country have similarly recognized that the Constitution protects the right to informational privacy. *E.g.*, *Hancock v. County of Rensselaer*, 882 F.3d 58, 65 (2d Cir. 2018); *In re Crawford*, 194 F.3d 954, 959 (9th Cir. 1999); *Woodland v. Houston*, 940 F.2d 134, 138 (5th Cir. 1991); *Pesce v. J. Sterling Morton High School*, 830 F.2d 789, 795-98 (7th Cir. 1987); *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 577-80 (3d Cir. 1980).

As courts have recognized, “individuals have an obvious privacy interest . . . in keeping secret the fact that they were subjects of a law enforcement investigation.” *National Magazine, Washington Bureau v. U.S. Customs Service*, 71 F.3d 885, 894 (D.C. Cir. 1995). The strength of this interest explains why grand jury proceedings are secret: to “assure that persons who are accused but exonerated by the grand jury will not be held up to public ridicule.” *Douglas Oil Co. v. Petrol Stops Northwest*, 441 U.S. 211, 219 (1979). This doctrine recognizes that individuals who are “investigated but not indicted” still suffer “adverse publicity” that invades their privacy. *Coughlan*, 842 F.2d at 739. The mere *fact* of criminal investigation creates a stigma that can effect a profound harm on an individual. *See Reporters Committee*, 489 U.S. at 767 (holding that individuals have a “significant privacy interest in their criminal histories”).

Compared with these substantial privacy interests, the public interest in disclosure here is minimal, if it exists at all. To be sure, the government and the public have a strong interest in ensuring that only qualified persons are registered to vote. *Greidinger*, 988 F.2d at 1354. For this very reason, the Board has undertaken a law-enforcement investigation of possible noncitizens on the voter rolls—which, in cases of verifiable voter fraud, may

lead to criminal prosecution. But publicly announcing the names of individuals whom the government has merely *investigated* for voter fraud does not further this interest. Indeed, because nearly all those persons have not, in fact, engaged in voter fraud, releasing their names would only undermine the integrity and credibility of the investigative process.

In sum, individuals have a weighty privacy interest against “disclosure of the fact that [they have] been under investigation.” *Douglas Oil*, 441 U.S. at 219. This privacy interest protects those “who are accused but exonerated” from the “public ridicule” of being unfairly suspected of a crime. *Id.* n.10. Thus, under the *Whalen* balancing test, disclosing the highly sensitive information requested by PILF would breach constitutional protections for informational privacy.

C. PILF’s Requests Are Also Invalid Because They Undermine Other Fundamental Constitutional Rights.

As just described, PILF’s requests intrude on constitutionally protected privacy rights. This intrusion on privacy is magnified in the situation here, where PILF’s requests also burden two other fundamental rights: the right to vote, and the right to be free from national-origin discrimination.

Informational privacy rights often help to secure other fundamental rights—rights like freedom of association, the right to vote, and equal protection of the laws. When a governmental invasion of privacy also imperils another fundamental right, courts subject that action to especially rigorous scrutiny.

For example, the Supreme Court has held that the First Amendment right to freedom of association cannot function effectively without “privacy in one’s associations.” *NAACP v. Alabama*, 357 U.S. 449, 462 (1958) (striking down a state law that required the NAACP to disclose its membership lists). As the Court explained, “privacy in group association” can be “indispensable” to freedom of association itself. *Id.* This is especially true when a group is subject to “public hostility.” *Id.*

Similarly, in *Greidinger*, this Court recognized that disclosure of a voter’s private information burdens voting rights. 988 F.2d 1344. In *Greidinger*, the Court held that requiring voters to publicly disclose personal information “place[s] a burdensome condition on the exercise of the fundamental right to vote” under the Equal Protection Clause. *Id.* at 1350. Moreover, because voting rights “preserve all other rights,” such disclosure

requirements must be narrowly drawn to advance a compelling government interest. *Id.* at 1348; *see id.* at 1350-52.

Thus, the Court applied “traditional equal protection strict scrutiny” to strike down a Virginia law that allowed for limited public disclosure of voters’ social security numbers. *Id.* at 1349, 1354-55. The Court made this ruling despite the significant safeguards that Virginia law imposed on access to voter information. For example, the law limited public access to a narrow group of persons, and required those persons to “sign an oath” promising to use the information for only specified purposes. *Id.* at 1345 & n.1. Even with these safeguards, the Court held that the law effected a “profound invasion of privacy” that could not be justified by any government interest. *Id.* at 1354.

Here, just as in *Greidinger*, PILF seeks to burden voting rights by imposing an onerous condition on the right to vote—the burden of being publicly branded as a potential felon. Indeed, courts have specifically held that when, as here, automated computer programs erroneously flag people as engaged in voter fraud, the Constitution bars disclosing those persons’

identities. *Moore v. Kobach*, 359 F.Supp.3d 1029, 1053-54 (D. Kan. 2019).⁸

That same result is warranted here.

But the constitutional harm here goes even further, because PILF's requests seek to burden voting rights selectively, in a way that harms a protected class. Specifically, PILF's requests disproportionately target naturalized citizens. As the experiences of other states show, the vast majority of persons who are flagged as potential noncitizen voters are recently naturalized citizens. These lawful voters are often listed erroneously as noncitizens in outdated government databases. *See supra*, at 5-8.

For this reason, courts have held that using automatically generated lists as proxies for noncitizen voting threatens the Equal Protection rights of naturalized citizens. *See Florida*, 870 F. Supp. 2d at 1347-48; *Whitley*, No. 5:19-cv-00074-FB, Doc. 61 at 4. After all, distinctions based on national origin are subject to strict scrutiny. *City of Cleburne, Tex. v. Cleburne Living Ctr.*, 473 U.S. 432, 440 (1985); *see* U.S. Const. am. XIV, § 1 ("All persons born

⁸ In *Kobach*, a group of lawful voters were publicly listed as potentially engaged in voter fraud, simply because they happened to share the same names and dates-of-birth as other registered voters. 359 F.Supp.3d at 1037-38. The court held that, by disclosing that list under a state public-records law, the state had violated the voters' right to informational privacy. *Id.*

or naturalized in the United States are citizens”); *Schneider v. Rusk*, 377 U.S. 163, 165 (1964) (“the rights of citizenship of the native born and of the naturalized person are of the same dignity and are coextensive”). Therefore, government actions that selectively expose recently naturalized citizens to public opprobrium are inherently suspect. *Zobel v. Williams*, 457 U.S. 55, 68-69 (1982) (Brennan, J., concurring) (observing that it violates Equal Protection to “discriminate against recently naturalized citizens”).

In sum, the privacy intrusions imposed by PILF’s requests undermine voting rights and selectively burden a protected class. These additional constitutional harms reinforce the conclusion that the Board was right to resist PILF’s demand that it disclose voters’ highly sensitive personal information.

At minimum, under the doctrine of constitutional avoidance, the district court was right to conclude that the information requested by PILF is protected by federal privacy laws.

CONCLUSION

Defendants respectfully request that this Court affirm the judgment below.

Respectfully submitted,

JOSHUA H. STEIN
Attorney General

/s/ Ryan Y. Park
Ryan Y. Park
Deputy Solicitor General

Caryn Devins Strickland
Solicitor General Fellow

Paul M. Cox
Special Deputy Attorney General

North Carolina Department of Justice
Post Office Box 629
Raleigh, North Carolina 27602
(919) 716-6400

February 12, 2020

CERTIFICATE OF SERVICE

I certify that on this 12th day of February, 2020, I filed this brief with the Clerk of Court using the CM/ECF system, which will automatically serve electronic copies on all counsel of record.

/s/ Ryan Y. Park

Ryan Y. Park

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because it contains 12,999 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f). This brief complies with the typeface and type-style requirements of Fed. R. App. P. 32(a)(5) & (6) because it has been prepared in a 14-point, proportionally spaced typeface.

/s/ Ryan Y. Park

Ryan Y. Park

- Addendum 1 -

CONTENTS OF ADDENDUM

	Addendum page
18 U.S.C. § 611	App. 2
52 U.S.C. § 20501	App. 4
52 U.S.C. § 20503(a)	App. 5
52 U.S.C. § 20504	App. 6
52 U.S.C. § 20505.....	App. 8
52 U.S.C. § 20506	App. 10
52 U.S.C. § 20507.....	App. 15
52 U.S.C. § 20508(b)	App. 25
18 U.S.C. §§ 2721(a)-(c)	App. 27
18 U.S.C. §§ 2725(1), (3)	App. 31
5 U.S.C. §§ 552a(a), (b), (m), (o)	App. 32

- Addendum 2 -

United States Code

Title 18.

Crimes and Criminal Procedure.

Part I.

Crimes.

Chapter 29.

Elections and Political Activities.

§ 611. Voting by aliens

- (a) It shall be unlawful for any alien to vote in any election held solely or in part for the purpose of electing a candidate for the office of President, Vice President, Presidential elector, Member of the Senate, Member of the House of Representatives, Delegate from the District of Columbia, or Resident Commissioner, unless--
 - (1) the election is held partly for some other purpose;
 - (2) aliens are authorized to vote for such other purpose under a State constitution or statute or a local ordinance; and
 - (3) voting for such other purpose is conducted independently of voting for a candidate for such Federal offices, in such a manner that an alien has the opportunity to vote for such other purpose, but not an opportunity to vote for a candidate for any one or more of such Federal offices.
- (b) Any person who violates this section shall be fined under this title, imprisoned not more than one year, or both.

- Addendum 3 -

- (c) Subsection (a) does not apply to an alien if--
- (1) each natural parent of the alien (or, in the case of an adopted alien, each adoptive parent of the alien) is or was a citizen (whether by birth or naturalization);
 - (2) the alien permanently resided in the United States prior to attaining the age of 16; and
 - (3) the alien reasonably believed at the time of voting in violation of such subsection that he or she was a citizen of the United States.

- Addendum 4 -

United States Code

Title 52.

Voting and Elections.

Subtitle II.

Voting Assistance and Election Administration.

Chapter 205.

National Voter Registration.

§ 20501. Findings and purposes.

(a) Findings

The Congress finds that--

- (1) the right of citizens of the United States to vote is a fundamental right;
- (2) it is the duty of the Federal, State, and local governments to promote the exercise of that right; and
- (3) discriminatory and unfair registration laws and procedures can have a direct and damaging effect on voter participation in elections for Federal office and disproportionately harm voter participation by various groups, including racial minorities.

(b) Purposes

The purposes of this chapter are—

- (1) to establish procedures that will increase the number of eligible citizens who register to vote in elections for

- Addendum 5 -

Federal office;

- (2) to make it possible for Federal, State, and local governments to implement this chapter in a manner that enhances the participation of eligible citizens as voters in elections for Federal office;
- (3) to protect the integrity of the electoral process; and
- (4) to ensure that accurate and current voter registration rolls are maintained.

§ 20503. National procedures for voter registration for elections for Federal office.

(a) In general

Except as provided in subsection (b), notwithstanding any other Federal or State law, in addition to any other method of voter registration provided for under State law, each State shall establish procedures to register to vote in elections for Federal office--

- (1) by application made simultaneously with an application for a motor vehicle driver's license pursuant to section 20504 of this title;
- (2) by mail application pursuant to section 20505 of this title; and
- (3) by application in person—
 - (A) at the appropriate registration site designated with respect to the residence of the applicant in accordance with State law; and
 - (B) at a Federal, State, or nongovernmental office designated under section 20506 of this title.

- Addendum 6 -

§ 20504. Simultaneous application for voter registration and application for motor vehicle driver's license

(a) In general

- (1) Each State motor vehicle driver's license application (including any renewal application) submitted to the appropriate State motor vehicle authority under State law shall serve as an application for voter registration with respect to elections for Federal office unless the applicant fails to sign the voter registration application.
- (2) An application for voter registration submitted under paragraph (1) shall be considered as updating any previous voter registration by the applicant.

(b) Limitation on use of information

No information relating to the failure of an applicant for a State motor vehicle driver's license to sign a voter registration application may be used for any purpose other than voter registration.

(c) Forms and procedures

- (1) Each State shall include a voter registration application form for elections for Federal office as part of an application for a State motor vehicle driver's license.
- (2) The voter registration application portion of an application for a State motor vehicle driver's license—
 - (A) may not require any information that duplicates information required in the driver's license portion of the form (other than a second signature or other information necessary under subparagraph (C));

- Addendum 7 -

- (B) may require only the minimum amount of information necessary to--
 - (i) prevent duplicate voter registrations; and
 - (ii) enable State election officials to assess the eligibility of the applicant and to administer voter registration and other parts of the election process;
- (C) shall include a statement that--
 - (i) states each eligibility requirement (including citizenship);
 - (ii) contains an attestation that the applicant meets each such requirement; and
 - (iii) requires the signature of the applicant, under penalty of perjury;
- (D) shall include, in print that is identical to that used in the attestation portion of the application—
 - (i) the information required in section 20507(a)(5)(A) and (B) of this title;
 - (ii) a statement that, if an applicant declines to register to vote, the fact that the applicant has declined to register will remain confidential and will be used only for voter registration purposes; and
 - (iii) a statement that if an applicant does register to vote, the office at which the applicant submits a voter registration application will remain confidential and will be used only for

- Addendum 8 -

voter registration purposes; and

- (E) shall be made available (as submitted by the applicant, or in machine readable or other format) to the appropriate State election official as provided by State law.

(d) Change of address

Any change of address form submitted in accordance with State law for purposes of a State motor vehicle driver's license shall serve as notification of change of address for voter registration with respect to elections for Federal office for the registrant involved unless the registrant states on the form that the change of address is not for voter registration purposes.

(e) Transmittal deadline

- (1) Subject to paragraph (2), a completed voter registration portion of an application for a State motor vehicle driver's license accepted at a State motor vehicle authority shall be transmitted to the appropriate State election official not later than 10 days after the date of acceptance.
- (2) If a registration application is accepted within 5 days before the last day for registration to vote in an election, the application shall be transmitted to the appropriate State election official not later than 5 days after the date of acceptance.

§ 20505. Mail registration

(a) Form

- (1) Each State shall accept and use the mail voter registration application form prescribed by the Federal Election Commission pursuant to section 20508(a)(2) of this title

- Addendum 9 -

for the registration of voters in elections for Federal office.

- (2) In addition to accepting and using the form described in paragraph (1), a State may develop and use a mail voter registration form that meets all of the criteria stated in section 20508(b) of this title for the registration of voters in elections for Federal office.
- (3) A form described in paragraph (1) or (2) shall be accepted and used for notification of a registrant's change of address.

(b) Availability of forms

The chief State election official of a State shall make the forms described in subsection (a) available for distribution through governmental and private entities, with particular emphasis on making them available for organized voter registration programs.

(c) First-time voters

- (1) Subject to paragraph (2), a State may by law require a person to vote in person if—
 - (A) the person was registered to vote in a jurisdiction by mail; and
 - (B) the person has not previously voted in that jurisdiction.
- (2) Paragraph (1) does not apply in the case of a person—
 - (A) who is entitled to vote by absentee ballot under the Uniformed and Overseas Citizens Absentee Voting Act;

- Addendum 10 -

- (B) who is provided the right to vote otherwise than in person under section 20102(b)(2)(B)(ii) of this title; or
 - (C) who is entitled to vote otherwise than in person under any other Federal law.
- (d) Undelivered notices

If a notice of the disposition of a mail voter registration application under section 20507(a)(2) of this title is sent by nonforwardable mail and is returned undelivered, the registrar may proceed in accordance with section 20507(d) of this title.

§ 20506. Voter registration agencies

- (a) Designation
 - (1) Each State shall designate agencies for the registration of voters in elections for Federal office.
 - (2) Each State shall designate as voter registration agencies—
 - (A) all offices in the State that provide public assistance; and
 - (B) all offices in the State that provide State-funded programs primarily engaged in providing services to persons with disabilities.
 - (3)(A) In addition to voter registration agencies designated under paragraph (2), each State shall designate other offices within the State as voter registration agencies.
 - (B) Voter registration agencies designated under subparagraph (A) may include--

- Addendum 11 -

- (i) State or local government offices such as public libraries, public schools, offices of city and county clerks (including marriage license bureaus), fishing and hunting license bureaus, government revenue offices, unemployment compensation offices, and offices not described in paragraph (2)(B) that provide services to persons with disabilities; and
 - (ii) Federal and nongovernmental offices, with the agreement of such offices.
- (4)(A) At each voter registration agency, the following services shall be made available:
 - (i) Distribution of mail voter registration application forms in accordance with paragraph (6).
 - (ii) Assistance to applicants in completing voter registration application forms, unless the applicant refuses such assistance.
 - (iii) Acceptance of completed voter registration application forms for transmittal to the appropriate State election official.
- (B) If a voter registration agency designated under paragraph (2)(B) provides services to a person with a disability at the person's home, the agency shall provide the services described in subparagraph (A) at the person's home.

- Addendum 12 -

- (5) A person who provides service described in paragraph (4) shall not—
 - (A) seek to influence an applicant's political preference or party registration;
 - (B) display any such political preference or party allegiance;
 - (C) make any statement to an applicant or take any action the purpose or effect of which is to discourage the applicant from registering to vote; or
 - (D) make any statement to an applicant or take any action the purpose or effect of which is to lead the applicant to believe that a decision to register or not to register has any bearing on the availability of services or benefits.
- (6) A voter registration agency that is an office that provides service or assistance in addition to conducting voter registration shall—
 - (A) distribute with each application for such service or assistance, and with each recertification, renewal, or change of address form relating to such service or assistance—
 - (i) the mail voter registration application form described in section 20508(a)(2) of this title, including a statement that—
 - (I) specifies each eligibility requirement (including citizenship);
 - (II) contains an attestation that the applicant meets each such requirement;

- Addendum 13 -

and

(III) requires the signature of the applicant, under penalty of perjury; or

(ii) the office's own form if it is equivalent to the form described in section 20508(a)(2) of this title,

unless the applicant, in writing, declines to register to vote;

(B) provide a form that includes—

(i) the question, “If you are not registered to vote where you live now, would you like to apply to register to vote here today?”;

(ii) if the agency provides public assistance, the statement, “Applying to register or declining to register to vote will not affect the amount of assistance that you will be provided by this agency.”;

(iii) boxes for the applicant to check to indicate whether the applicant would like to register or declines to register to vote (failure to check either box being deemed to constitute a declination to register for purposes of subparagraph (C)), together with the statement (in close proximity to the boxes and in prominent type), “IF YOU DO NOT CHECK EITHER BOX, YOU WILL BE CONSIDERED TO HAVE DECIDED NOT TO REGISTER TO VOTE AT THIS TIME.”;

- Addendum 14 -

- (iv) the statement, “If you would like help in filling out the voter registration application form, we will help you. The decision whether to seek or accept help is yours. You may fill out the application form in private.”; and
 - (v) the statement, “If you believe that someone has interfered with your right to register or to decline to register to vote, your right to privacy in deciding whether to register or in applying to register to vote, or your right to choose your own political party or other political preference, you may file a complaint with _____.”, the blank being filled by the name, address, and telephone number of the appropriate official to whom such a complaint should be addressed; and
 - (C) provide to each applicant who does not decline to register to vote the same degree of assistance with regard to the completion of the registration application form as is provided by the office with regard to the completion of its own forms, unless the applicant refuses such assistance.
- (7) No information relating to a declination to register to vote in connection with an application made at an office described in paragraph (6) may be used for any purpose other than voter registration.
- (b) Federal Government and private sector cooperation

All departments, agencies, and other entities of the executive branch of the Federal Government shall, to the greatest extent practicable, cooperate with the States in carrying out subsection (a), and all nongovernmental entities are encouraged to do so.

- Addendum 15 -

(c) Armed Forces recruitment offices

- (1) Each State and the Secretary of Defense shall jointly develop and implement procedures for persons to apply to register to vote at recruitment offices of the Armed Forces of the United States.
- (2) A recruitment office of the Armed Forces of the United States shall be considered to be a voter registration agency designated under subsection (a)(2) for all purposes of this chapter.

(d) Transmittal deadline

- (1) Subject to paragraph (2), a completed registration application accepted at a voter registration agency shall be transmitted to the appropriate State election official not later than 10 days after the date of acceptance.
- (2) If a registration application is accepted within 5 days before the last day for registration to vote in an election, the application shall be transmitted to the appropriate State election official not later than 5 days after the date of acceptance.

§ 20507. Requirements with respect to administration of voter registration

(a) In general

In the administration of voter registration for elections for Federal office, each State shall—

- (1) ensure that any eligible applicant is registered to vote in an election—
 - (A) in the case of registration with a motor vehicle

- Addendum 16 -

application under section 20504 of this title, if the valid voter registration form of the applicant is submitted to the appropriate State motor vehicle authority not later than the lesser of 30 days, or the period provided by State law, before the date of the election;

(B) in the case of registration by mail under section 20505 of this title, if the valid voter registration form of the applicant is postmarked not later than the lesser of 30 days, or the period provided by State law, before the date of the election;

(C) in the case of registration at a voter registration agency, if the valid voter registration form of the applicant is accepted at the voter registration agency not later than the lesser of 30 days, or the period provided by State law, before the date of the election; and

(D) in any other case, if the valid voter registration form of the applicant is received by the appropriate State election official not later than the lesser of 30 days, or the period provided by State law, before the date of the election;

(2) require the appropriate State election official to send notice to each applicant of the disposition of the application;

(3) provide that the name of a registrant may not be removed from the official list of eligible voters except—

(A) at the request of the registrant;

(B) as provided by State law, by reason of criminal conviction or mental incapacity; or

- Addendum 17 -

- (C) as provided under paragraph (4);
 - (4) conduct a general program that makes a reasonable effort to remove the names of ineligible voters from the official lists of eligible voters by reason of—
 - (A) the death of the registrant; or
 - (B) a change in the residence of the registrant, in accordance with subsections (b), (c), and (d);
 - (5) inform applicants under sections 20504, 20505, and 20506 of this title of—
 - (A) voter eligibility requirements; and
 - (B) penalties provided by law for submission of a false voter registration application; and
 - (6) ensure that the identity of the voter registration agency through which any particular voter is registered is not disclosed to the public.
- (b) Confirmation of voter registration

Any State program or activity to protect the integrity of the electoral process by ensuring the maintenance of an accurate and current voter registration roll for elections for Federal office—

- (1) shall be uniform, nondiscriminatory, and in compliance with the Voting Rights Act of 1965 (42 U.S.C. 1973 et seq.); and
- (2) shall not result in the removal of the name of any person from the official list of voters registered to vote in an election for Federal office by reason of the person's failure

- Addendum 18 -

to vote, except that nothing in this paragraph may be construed to prohibit a State from using the procedures described in subsections (c) and (d) to remove an individual from the official list of eligible voters if the individual—

- (A) has not either notified the applicable registrar (in person or in writing) or responded during the period described in subparagraph (B) to the notice sent by the applicable registrar; and then
- (B) has not voted or appeared to vote in 2 or more consecutive general elections for Federal office.

(c) Voter removal programs

- (1) A State may meet the requirement of subsection (a)(4) by establishing a program under which—
 - (A) change-of-address information supplied by the Postal Service through its licensees is used to identify registrants whose addresses may have changed; and
 - (B) if it appears from information provided by the Postal Service that—
 - (i) a registrant has moved to a different residence address in the same registrar's jurisdiction in which the registrant is currently registered, the registrar changes the registration records to show the new address and sends the registrant a notice of the change by forwardable mail and a postage prepaid pre-addressed return form by which the registrant may verify or correct the address information; or

- Addendum 19 -

- (ii) the registrant has moved to a different residence address not in the same registrar's jurisdiction, the registrar uses the notice procedure described in subsection (d)(2) to confirm the change of address.
- (2)(A) A State shall complete, not later than 90 days prior to the date of a primary or general election for Federal office, any program the purpose of which is to systematically remove the names of ineligible voters from the official lists of eligible voters.
- (B) Subparagraph (A) shall not be construed to preclude—
 - (i) the removal of names from official lists of voters on a basis described in paragraph (3)(A) or (B) or (4)(A) of subsection (a); or
 - (ii) correction of registration records pursuant to this chapter.
- (d) Removal of names from voting rolls
 - (1) A State shall not remove the name of a registrant from the official list of eligible voters in elections for Federal office on the ground that the registrant has changed residence unless the registrant—
 - (A) confirms in writing that the registrant has changed residence to a place outside the registrar's jurisdiction in which the registrant is registered; or
 - (B)(i) has failed to respond to a notice described in paragraph (2); and

- Addendum 20 -

- (ii) has not voted or appeared to vote (and, if necessary, correct the registrar's record of the registrant's address) in an election during the period beginning on the date of the notice and ending on the day after the date of the second general election for Federal office that occurs after the date of the notice.
- (2) A notice is described in this paragraph if it is a postage prepaid and pre-addressed return card, sent by forwardable mail, on which the registrant may state his or her current address, together with a notice to the following effect:
 - (A) If the registrant did not change his or her residence, or changed residence but remained in the registrar's jurisdiction, the registrant should return the card not later than the time provided for mail registration under subsection (a)(1)(B). If the card is not returned, affirmation or confirmation of the registrant's address may be required before the registrant is permitted to vote in a Federal election during the period beginning on the date of the notice and ending on the day after the date of the second general election for Federal office that occurs after the date of the notice, and if the registrant does not vote in an election during that period the registrant's name will be removed from the list of eligible voters.
 - (B) If the registrant has changed residence to a place outside the registrar's jurisdiction in which the registrant is registered, information concerning how the registrant can continue to be eligible to vote.
- (3) A voting registrar shall correct an official list of eligible voters in elections for Federal office in accordance with

- Addendum 21 -

change of residence information obtained in conformance with this subsection.

- (e) Procedure for voting following failure to return card
 - (1) A registrant who has moved from an address in the area covered by a polling place to an address in the same area shall, notwithstanding failure to notify the registrar of the change of address prior to the date of an election, be permitted to vote at that polling place upon oral or written affirmation by the registrant of the change of address before an election official at that polling place.
 - (2)(A) A registrant who has moved from an address in the area covered by one polling place to an address in an area covered by a second polling place within the same registrar's jurisdiction and the same congressional district and who has failed to notify the registrar of the change of address prior to the date of an election, at the option of the registrant—
 - (i) shall be permitted to correct the voting records and vote at the registrant's former polling place, upon oral or written affirmation by the registrant of the new address before an election official at that polling place; or
 - (ii)(I) shall be permitted to correct the voting records and vote at a central location within the same registrar's jurisdiction designated by the registrar where a list of eligible voters is maintained, upon written affirmation by the registrant of the new address on a standard form provided by the registrar at the central location; or

- Addendum 22 -

- (II) shall be permitted to correct the voting records for purposes of voting in future elections at the appropriate polling place for the current address and, if permitted by State law, shall be permitted to vote in the present election, upon confirmation by the registrant of the new address by such means as are required by law.
- (B) If State law permits the registrant to vote in the current election upon oral or written affirmation by the registrant of the new address at a polling place described in subparagraph (A)(i) or (A)(ii)(II), voting at the other locations described in subparagraph (A) need not be provided as options.
- (3) If the registration records indicate that a registrant has moved from an address in the area covered by a polling place, the registrant shall, upon oral or written affirmation by the registrant before an election official at that polling place that the registrant continues to reside at the address previously made known to the registrar, be permitted to vote at that polling place.
- (f) Change of voting address within a jurisdiction

In the case of a change of address, for voting purposes, of a registrant to another address within the same registrar's jurisdiction, the registrar shall correct the voting registration list accordingly, and the registrant's name may not be removed from the official list of eligible voters by reason of such a change of address except as provided in subsection (d).
- (g) Conviction in Federal court
 - (1) On the conviction of a person of a felony in a district

- Addendum 23 -

court of the United States, the United States attorney shall give written notice of the conviction to the chief State election official designated under section 20509 of this title of the State of the person's residence.

- (2) A notice given pursuant to paragraph (1) shall include—
 - (A) the name of the offender;
 - (B) the offender's age and residence address;
 - (C) the date of entry of the judgment;
 - (D) a description of the offenses of which the offender was convicted; and
 - (E) the sentence imposed by the court.
- (3) On request of the chief State election official of a State or other State official with responsibility for determining the effect that a conviction may have on an offender's qualification to vote, the United States attorney shall provide such additional information as the United States attorney may have concerning the offender and the offense of which the offender was convicted.
- (4) If a conviction of which notice was given pursuant to paragraph (1) is overturned, the United States attorney shall give the official to whom the notice was given written notice of the vacation of the judgment.
- (5) The chief State election official shall notify the voter registration officials of the local jurisdiction in which an offender resides of the information received under this subsection.

(h) Omitted

- Addendum 24 -

(i) Public disclosure of voter registration activities

- (1) Each State shall maintain for at least 2 years and shall make available for public inspection and, where available, photocopying at a reasonable cost, all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters, except to the extent that such records relate to a declination to register to vote or to the identity of a voter registration agency through which any particular voter is registered.
- (2) The records maintained pursuant to paragraph (1) shall include lists of the names and addresses of all persons to whom notices described in subsection (d)(2) are sent, and information concerning whether or not each such person has responded to the notice as of the date that inspection of the records is made.

(j) “Registrar's jurisdiction” defined

For the purposes of this section, the term “registrar's jurisdiction” means—

- (1) an incorporated city, town, borough, or other form of municipality;
- (2) if voter registration is maintained by a county, parish, or other unit of government that governs a larger geographic area than a municipality, the geographic area governed by that unit of government; or
- (3) if voter registration is maintained on a consolidated basis for more than one municipality or other unit of government by an office that performs all of the functions of a voting registrar, the geographic area of the

- Addendum 25 -

consolidated municipalities or other geographic units.

§ 20508. Federal coordination and regulations

...

(b) Contents of mail voter registration form

The mail voter registration form developed under subsection (a)(2)—

- (1) may require only such identifying information (including the signature of the applicant) and other information (including data relating to previous registration by the applicant), as is necessary to enable the appropriate State election official to assess the eligibility of the applicant and to administer voter registration and other parts of the election process;
- (2) shall include a statement that—
 - (A) specifies each eligibility requirement (including citizenship);
 - (B) contains an attestation that the applicant meets each such requirement; and
 - (C) requires the signature of the applicant, under penalty of perjury;
- (3) may not include any requirement for notarization or other formal authentication; and
- (4) shall include, in print that is identical to that used in the attestation portion of the application—
 - (i) the information required in section 20507(a)(5)(A)

- Addendum 26 -

and (B) of this title;

- (ii) a statement that, if an applicant declines to register to vote, the fact that the applicant has declined to register will remain confidential and will be used only for voter registration purposes; and
- (iii) a statement that if an applicant does register to vote, the office at which the applicant submits a voter registration application will remain confidential and will be used only for voter registration purposes.

- Addendum 27 -

United States Code

Title 18.

Crimes and Criminal Procedure.

Part I.

Crimes.

Chapter 123.

**Prohibition on Release and Use of Certain Personal Information from
State Motor Vehicle Records.**

**§ 2721. Prohibition on release and use of certain personal
information from State motor vehicle records**

- (a) In general.--A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity:
 - (1) personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section; or
 - (2) highly restricted personal information, as defined in 18 U.S.C. 2725(4), about any individual obtained by the department in connection with a motor vehicle record, without the express consent of the person to whom such information applies, except uses permitted in subsections (b)(1), (b)(4), (b)(6), and (b)(9): Provided, That subsection (a)(2) shall not in any way affect the use of organ donation information on an individual's driver's license or affect the administration of organ donation

- Addendum 28 -

initiatives in the States.

- (b) Permissible uses.--Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. 1231 et seq.), the Clean Air Act (42 U.S.C. 7401 et seq.), and chapters 301, 305, and 321-331 of title 49, and, subject to subsection (a)(2), may be disclosed as follows:
- (1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.
 - (2) For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.
 - (3) For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only—
 - (A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and

- Addendum 29 -

- (B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
- (4) For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.
- (5) For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.
- (6) For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.
- (7) For use in providing notice to the owners of towed or impounded vehicles.
- (8) For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.
- (9) For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.
- (10) For use in connection with the operation of private toll

- Addendum 30 -

transportation facilities.

- (11) For any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains.
 - (12) For bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.
 - (13) For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.
 - (14) For any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety.
- (c) Resale or redisclosure.--An authorized recipient of personal information (except a recipient under subsection (b)(11) or (12)) may resell or redisclose the information only for a use permitted under subsection (b) (but not for uses under subsection (b) (11) or (12)). An authorized recipient under subsection (b)(11) may resell or redisclose personal information for any purpose. An authorized recipient under subsection (b)(12) may resell or redisclose personal information pursuant to subsection (b)(12). Any authorized recipient (except a recipient under subsection (b)(11)) that resells or rediscloses personal information covered by this chapter must keep for a period of 5 years records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle department upon request.

...

- Addendum 31 -

§ 2725. Definitions

In this chapter—

- (1) “motor vehicle record” means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles;

...

- (3) “personal information” means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.

...

- Addendum 32 -

United States Code

Title 5.

Government Organization and Employees.

Part I.

The Agencies Generally.

Chapter 5.

Administrative Procedure.

Subchapter II.

Administrative Procedure.

§ 552a. Records maintained on individuals.

(a) Definitions.--For purposes of this section—

...

- (4) the term “record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;
- (5) the term “system of records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying

- Addendum 33 -

particular assigned to the individual;

...

- (b) Conditions of disclosure.--No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be—
- (1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
 - (2) required under section 552 of this title;
 - (3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;
 - (4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;
 - (5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
 - (6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;

- Addendum 34 -

- (7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
- (8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
- (9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
- (10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the Government Accountability Office;
- (11) pursuant to the order of a court of competent jurisdiction;
or
- (12) to a consumer reporting agency in accordance with section 3711(e) of title 31.

...

- (m)(1) Government contractors.--When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such

- Addendum 35 -

contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

...

- (o) Matching agreements.--(1) No record which is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency specifying—
 - (A) the purpose and legal authority for conducting the program;
 - (B) the justification for the program and the anticipated results, including a specific estimate of any savings;
 - (C) a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;
 - (D) procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)), to—
 - (i) applicants for and recipients of financial assistance or payments under Federal benefit programs, and
 - (ii) applicants for and holders of positions as Federal

- Addendum 36 -

personnel,

that any information provided by such applicants, recipients, holders, and individuals may be subject to verification through matching programs;

- (E) procedures for verifying information produced in such matching program as required by subsection (p);
- (F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;
- (G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;
- (H) prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;
- (I) procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;
- (J) information on assessments that have been made on the accuracy of the records that will be used in such matching program; and
- (K) that the Comptroller General may have access to all records of a recipient agency or a non-Federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.

- Addendum 37 -

- (2)(A) A copy of each agreement entered into pursuant to paragraph (1) shall—
- (i) be transmitted to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives; and
 - (ii) be available upon request to the public.
- (B) No such agreement shall be effective until 30 days after the date on which such a copy is transmitted pursuant to subparagraph (A)(i).
- (C) Such an agreement shall remain in effect only for such period, not to exceed 18 months, as the Data Integrity Board of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct, of the matching program.
- (D) Within 3 months prior to the expiration of such an agreement pursuant to subparagraph (C), the Data Integrity Board of the agency may, without additional review, renew the matching agreement for a current, ongoing matching program for not more than one additional year if—
- (i) such program will be conducted without any change; and
 - (ii) each party to the agreement certifies to the Board in writing that the program has been conducted in compliance with the agreement.